

63/5401/95A

COAST GUARD
27A

TOP SECRET

05

1/25

Reviewed for declassification in accordance with
Executive Order 12065 on 2 OCT 1980
(Date)

Present classification and special handling requirements:
(refer to automated Depository Index System)

U = UNCLASSIFIED	0 = For Official Use Only
	1 = Special Intelligence
C = CONFIDENTIAL	(2) = SI Codeword
	3 = SNCP
S = SECRET	4 = PW
	5 = SAO
(T) = TOP SECRET	6 = PA Information
	7 = FOIA Exemption

Reason for extension of classification (if applicable):

<input checked="" type="checkbox"/>	Foreign Government Information
<input checked="" type="checkbox"/>	Intelligence sources, methods, activities
<input checked="" type="checkbox"/>	Cryptographic information
<input type="checkbox"/>	Foreign Relations/Activities
<input type="checkbox"/>	Scientific/Technological Material
<input type="checkbox"/>	Military Plans, Weapons, Operations

AUTHORITY: R. P. Schmidt

Next scheduled review date: OCT 2000

History of Coast Guard Unit # 387, 1940-1945

TOP SECRET ULTRA

HISTORY
OF
COAST GUARD UNIT #387
1940-1945

COPY	#1 - OP-20-G
"	2 - ARMY
"	3 - BRITISH
"	4 - CAPT. F.E. POLLIO
"	5 - OP-20-3-GH

TOP SECRET ULTRA

OUTLINE

Foreword

PART I. Hand-Operated Systems

A. Early Systems

1. Introductory
2. Code Systems
 - a. Enciphered Commercial Code
 - b. Dictionary Code

B. Simple Substitution

1. Monoalphabetic Substitution
 - a. 4-A Hamburg-England
 - b. 4-AL Madrid-Cape Spartel
2. Polyalphabetic Substitution - Periodic
 - a. 3-I Hamburg-Rio de Janeiro
 - b. 6-A Shanghai-Canton

C. Nonperiodic Substitution: Running Key

1. 3-G Hamburg-Valparaiso
2. 4-F Hamburg-Lisbon
3. 3-J Hamburg-South America
4. 5-D Hamburg-The Crimea

D1 Single Transposition: Columnar

a. Hamburg Center

1. 2-B Hamburg-New York
2. 3-C Hamburg-Valparaiso
3. 3-A Hamburg-Rio de Janeiro
4. 3-B Hamburg-Rio de Janeiro
5. 3-D Germany-Rio de Janeiro
6. 3-E Bremen-Rio de Janeiro
7. 5-C Hamburg-Ankara
8. 4-I Hamburg-Bordeaux
9. 4-H Hamburg-Unknown

TOP SECRET ULTRA

b. Lisbon Center

1. 4-G Lisbon-Portuguese Guinea
2. 4-C Lisbon-Lourenco Marques

c. Stuttgart Center

1. 4-C Stuttgart-Libya

D2 Single Transposition: Combs

1. 3-F Cologne-Rio de Janeiro
2. 3-H Hamburg-Sao Paulo
3. 4-E Hamburg-Lisbon

D3 Single Transposition: Grilles

1. Brajob-Volco Circuit, Berlin-Mexico and
2-B Berlin-Mexico
2. 3-D Berlin-Rio de Janeiro
3. 4-D Madrid-West Africa

E. Single Transposition-Substitution

E1. Monoalphabetic Substitution with Comb Transposition

4-N Hamburg-Unknown

E2. Polyalphabetic Substitution with trivial Transposition

4-I Hamburg-Bordeaux

E3. Polyalphabetic Substitution with Columnar Transposition Janowski Method

1. 4-M Hamburg-Spain
2. 4-L Hamburg-Gijon
3. 4-P Hamburg-Madrid
4. 4-F Hamburg-Lisbon
5. 4-R Hamburg-Vigo
6. 4-Q Hamburg-Tangier
7. 4-I Hamburg-Bordeaux

F. Double Transposition

1. 4-Q Berlin-Madrid
2. 4-S Berlin-Tetuan
3. 4-T Berlin-Teheran
4. 3-N Berlin-Argentina

TOP SECRET ULTRA

3. Double Transposition-Substitution: Post-Weaver Systems
 1. Introductory: Cryptographic Features of "ABC SCHLUESSEL."
 2. Solution: ABC SCHLUESSEL
 - a. Reconstruction of the Substitution Alphabet
 - b. Solution of the Transposition Key
 - G(1). Solution by means of a complete crib.
Circuit U-L1, Hamburg-Spain.
 - G(2). Solution by means of a partial crib.
L-R Hamburg-Vigo
 - G(3). Solution of case where both transposition keys are the same. L-X Hamburg-Lisbon
 - G(4). Solution by decipher of message in which one step was omitted. L-P Berlin-Madrid
 - G(5). Solution by Key Weights
3. Procedure 62
 - a. Introductory
 - b. Cryptographic Features of Procedure 62
 - c. Solution
 - (1). Solution by means of a decipher
 - (2). Solution by means of a complete crib
4. Procedure 40
 - a. Cryptographic Features
 - b. Solution of L-AD Madrid-Centa

PART II. Devices and Machines

A. Schluesselrad

1. Device used in Chile
2. Device used by Jolle with Argentine Station

B. Kryha

1. History
2. Solution
3. Later Developments

TOP SECRET ULTRA

C. Enigma: Wheel Wiring Unknown

1. Single Turnover. MAN-RDA-NDR
2. Multiple Turnover Green Machine
 - a. History
 - b. Solution
 - c. Recovery of Wheel wiring
3. Red Machine
 - a. History
 - b. Solution
 - c. Recovery of Wheel wiring for Wheels
 - d. Removal of the Twist

D. Determination of the Use of Known Wheels on Unsolved Circuits

1. Multiple Turnover Wheels. 4-O Berlin-Madrid
2. Stecker. 4-I Hamburg-Bordeaux

Chart of Hamburg Center Networks

Chart of Berlin Center Networks

TOP SECRET ULYAN

FOREWORD

The Coast Guard Cryptanalytic Unit was established in 1931 for the purpose of solving messages passing between groups of smugglers and other criminals violating statutes enforced by law enforcement agencies of the Treasury Department. In monitoring illegal radio networks during the prohibition era (1927-1934) Coast Guard monitors became proficient in recognizing and following unauthorized stations. After the outbreak of the War in Europe in September, 1939, the Coast Guard continued its monitoring activities for the purpose of detecting possible unneutral communications affecting shipping and the movements of vessels of belligerent nations or any communications indicating violation of any of the neutrality laws then enforced by the Treasury Department.

In the course of the latter monitoring activities Coast Guard monitors repeatedly submitted intercepts from stations whose operating procedures and characteristics were in many respects similar to those so frequently heard on the air during the smuggling era. The solution of some of these messages revealed that the stations whose transmissions were being copied were engaged in espionage operations.

The Coast Guard continued the interception and solution of this new type of traffic, forwarding solutions to the interested United States government agencies, including the Federal Bureau of Investigation. Following this, a number of requests were received from the Federal Bureau of Investigation for assistance in solution of suspicious messages which proved to be of the same origin.

On 1 November, 1941, the Coast Guard was transferred from the Treasury Department to the Navy. A few months thereafter the Coast Guard Cryptanalytic Unit started operating as a part of Op-20-G.

On 30 June, 1942, by an agreement entered into by the Army, Navy and the Federal Bureau of Investigation, the arrangement which had been in effect more or less unofficially by virtue of mutual consent, was made official and the clandestine field, outside the Western Hemisphere, was assigned to the Coast Guard and within the Western Hemisphere to the Coast Guard and the Federal Bureau of Investigation jointly.

TOP SECRET ULTRA

Because of the fact that no historical records of cryptanalytic procedures were maintained during the years the Coast Guard Unit functioned in the clandestine field, and since, therefore, this history will be the only document of record, the descriptions herein of earlier solutions are much more detailed than is warranted by the simplicity of the systems discussed. Such portions are therefore of interest to the historian rather than to the cryptanalyst.

TOP SECRET ULTRA

PART I. HAND-OPERATED SYSTEMS

A. EARLY SYSTEMS

1. INTRODUCTORY

Following the outbreak of war in Europe, Coast Guard monitors were directed to cover commercial transmissions passing between North and South America.

Numerous cases using enciphered commercial code appeared, emanating from Axis dominated commercial firms in Mexico and Central and South America.

After the entry of the United States into the war, and the breaking of diplomatic relations with the Axis by most of the Central and South American countries, a tight censorship caused the cessation of practically all such traffic.

2. CODE SYSTEMS

a. ENCIPHERED COMMERCIAL CODE

The most significant exchange of messages in this category became known to this office as the OPALU messages.

Between July, 1941 and April, 1942, traffic passing between Hamburg, Berlin and Mexico used the Rudolph Mosse Code with the letters of the group transposed and a substitution on the last two letters of the group. The following addresses were used: From Hamburg to Sudamero, Mexico and Sudameriat, Mexico; and from Mexico to Sudameriat, Hamburg, Sudamvorst, Berlin, Sudamero, Berlin, and Sudameriat, Berlin.

The indicator OPALU was usually sent as the first group of the message. The substitution alphabet for the last two letters of the group was as follows:

Cipher: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Plain: U C D B A G H F O N M K J L E T Q V W R Y X Z S I P

The transposition key was: 3 4 5 1 2

TOP SECRET ULTRA

Example:

Message: OPALU SOHEP EXEHU OLICV ESELM, etc.

- (a) Transposition: SOHEP -- HEP SO
EXEHU -- EHUEX
OLICV -- ICVOL
ESELM -- ELMES
- (b) Substitution: HEP SO -- HEPWE
EHUEX -- EHUA S
ICVOL -- ICVEK
ELMES -- ELMAN
- (c) Decode: HEPWE -- Business manager
EHUA S -- German
ICVEK -- Chamber of Commerce
ELMAN -- Colon

In August, 1941 traffic from SOLINGEN, Nauen to BOKER, Mexico used the Rudolph Mosse Code with a subtractor of seven.

Messages originating in Mexico using the cable address MUENCH-IMPO, Hamburg, in 1941, employed a mixed arrangement within the messages of the Rudolph Mosse and Peterson Codes.

Other cable communications employed Acme, Peterson, Mosse or Alpha Codes, either in combination with each other, or with simple forms of encipherment.

TOP SECRET ULTRA

b. DICTIONARY CODE

Traffic on this circuit was transmitted over the commercial MEXICO-NAMEN circuit and the first message was intercepted on 1 January, 1940.

This traffic contained only the following 11 letters of the alphabet, with the letter N occurring most frequently; N, R, H, A, D, K, U, C, W, E, and L. This suggested that a key word was being used for letter-number substitution, with the letter N serving as a separator. By anagramming these 11 letters the word DURCHWALKEN was derived. The key was then:

D U R C H W A L K E N
1 2 3 4 5 6 7 8 9 0 -

For example, a message sent as

UHHNR LNDAL NURND WCNCK NPHLN DNFRAN CHNDR UNDEN, etc.

would become

255-38 178-23 164-49 358-1 37-45 132-10, etc.

It was assumed that these figures represented page and line numbers of a dictionary, possibly a German-Spanish dictionary, and from the range of page and number of words per page, was considered likely to be a small or pocket-size book.

After several messages had been intercepted and converted to figures, it was noted that some combinations of figures occurred more frequently than others. From this it was surmised that these combinations represented either numerals or letters of the alphabet.

The code groups 1-1, 132-10, 343-2, 65-12, 375-2 and 321-2 appeared with greater frequency than any other groups. These groups were underlined wherever they appeared in the messages available, in an attempt to bracket and identify other letter equivalents and thus isolate sections of spelling.

Several messages sent during the early part of 1941 had the following ending which seemed to be some sort of signature:

TOP SECRET ULTRA

65-12 375-2 132-10 321-2 132-10 343-2

Another message contained the following:

65-12 132-10 373-2 301-21 285-25 343-2

These were selected for study and after a little experimenting the following was produced:

65-12 132-10 373-2 301-21 285-25 343-2
B E R L I N

65-12 375-2 132-10 321-2 132-10 343-2
B R E M E N

Insertion of these values in all messages led to the identification of the words "MAX" and "GLENN", the names of two known German agents, and brought out portions of names which appeared to be ship names. Perusal of shipping publications revealed names of ships in Chilean ports, on appropriate dates, which identified a number of these partial names.

The complete alphabet was approximately as follows:

A - 1-1	N - 343-2
B - 65-13	O - 353-27
C - 112-1	P - 358-1
D - 113-23	Q - 373-21
E - 132-10	R - 375-1
F - 165-6	S - 391-26
G - 191-30	T - 449-16
H - 227-1	U - 464-1
I - 258-25	V - 486-22
J - 263-49	W - 514-18
K - 267-4	X - 535-4
L - 301-21	Y - 535-9
M - 321-1	Z - 535-10

The above table is not complete because occasionally there were several values for a letter in cases where the beginning of its alphabetic block contained several variant forms of the single letter.

TOP SECRET ULTRA

With the alphabet recovered and the vocabulary divided into alphabetic blocks, whole words were identified. Messages containing ship names afforded most opportunities for identifications, since in this type of message words were used involving arrival and departure dates, types of cargo loaded and discharged, etc.

Most of the shipping messages were read completely because of the limited phraseology. Other messages were read partially, and the meaning expanded as later messages brought out additional identifications of the plain text words.

In March, 1941 another key word, CONVERSATION, was used for the substitution. The substitution key CEGIKMOQSUN was used on 17 June, 1941 and ACEGIKMOQSU on 5 June, 1941. Although these two keys were used only once each, they were easily recovered.

All of the messages in 1940 and 1941 were sent with the heading SUDAMERIAT, WEDEKIND, SUDAMERO, or EGMARSUD.

In March, 1942 traffic was transmitted from Chile with the cable address BACOHASE and the messages signed SCHOEN, who was the German ambassador to Chile. The key word was AUSWIRKEND, which was later changed to ZYKLOPISCH. For these two keys, however, all other letters of the alphabet were used for a separator between the page and line numbers.

Eventually the dictionary being used for encoding these messages was found and was used to decode the messages. The title was "LANGENSCHIEDTS TASCHENWOERTERBUCH der spanischen und deutschen Sprache." All messages were completely decoded after a copy of the dictionary became available.

TOP SECRET ULTRA

B. SIMPLE SUBSTITUTION

1. MONOALPHABETIC SUBSTITUTION

a. 4-A HAMBURG-ENGLAND

In October, 1940, the monitors intercepted transmissions from a suspicious station. The traffic sent by this station was in five-letter groups and was prefaced by a preamble consisting of two four-letter groups and two three-letter groups. This station used the chatter that was typical of American "ham" operators, and it also utilized a series of calls which changed every day and which were in an alphabetical progression, i.e., ACE, BDF, CEI, etc. On 18 October, 1940 this station transmitted:

HR CODE FROM YESTERDAY FROM 17 OF OCTOBER

CTCP PNVP CCP PPC

HBOOP QHSMW QLQKM EGOEL, etc.

The preamble was tried for a monoalphabetic substitution of letter for figure, which proved to be correct:

CTCP PNVP CCP PPC
1710 0940 110 001

When the traffic was tested, it also exhibited a frequency count of monoalphabetic substitution. Solution was as follows:

HBOOP QHSMW QLQKM EGOEL, etc.
HATTE NHOFF NUNGF ASTAU

The preamble key, called "Zahlschlüssel" by the Germans, was also used in the plain text to indicate numbers, i.e.,

UM X CCPP X UHR
UM X 1100 X UHR

The traffic usually ended with an incomplete final group of cipher text. The call letters, preamble key, and substitution key all were changed daily, the day of the month controlling the progression of the normal alphabet through a Vigenere square.

TOP SECRET ULTRA

When the traffic was deciphered, it was discovered that the plain text was in German, and that the messages emanated from a station in Germany sending out requests for information from an agent in England. Sometime later it was learned that the agent had been seized and his station taken over by the British.

b. 4-AL MADRID-CAPE SPARTEL

In January, 1945, traffic from this circuit was first intercepted by Coast Guard monitors. The first message intercepted was quite obviously in monoalphabetic substitution due to the number of repeats in the cipher text, and the frequency distribution which, merely from usual inspection was patently monoalphabetic.

The plain text was Spanish, principally reports of convoys sighted off Cape Spartel.

Although all messages for one day employed the same substitution alphabet, there appeared to be eight different monoalphabets. These were used in a regular day-by-day progression, the same one being used every eighth day. Messages enciphered by seven of these monoalphabets were intercepted, but traffic from the eighth day in the cycle was never intercepted.

The components of the substitution alphabets contained 26 letters, but, in each there was no W -- the Spanish Ñ being inserted between N and O of the normal alphabet to form the plain component. The cipher component in each case was apparently formed by performing some trivial (rail-fencing or decimating) transposition on the plain component.

TOP SECRET ULTRA

2. POLYALPHABETIC SUBSTITUTION-FEUTODIV

a. 3-I HAMBURG-RIO DE JANEIRO

In October, 1941, a circuit was discovered in which the control station used the constant call sign and the answer station RND. The traffic had a preamble in which the date and month and group check were given outside the cipher text, i.e.,

0904

h2

the first group indicating April 9th, the second group indicating h2 groups in the message. the traffic was examined, and the frequency count showed characteristics of polyalphabetic substitution. Further inspection revealed long repeats, i.e.,

DLUX C SFV INENW FRFZA QQRDI
WREKU ZPRIY HUXFS JRUJP TYARH
SARWC QQFYD MLXP VHJRE KMLIJ
WQJAI JYNPV USQLJ DHOIV HJORN
HSJRU VJKT NPPBI SEKRV OIVGC
GQBS NUPAS FVHJU WRFPS PTACT
FSXJQ FWJW UNFTC JIMHH PJHQB
HUVFE DPJRF AFAVH URBNQ TLDLU
ACSD ESXU

It will be noted that there is a six-letter repeat (DLUXCQ) and a three-letter repeat (OIV), plus two two-letter repeats. There are 196 letters between the six-letter repeat and 23 letters between the three-letter repeat, both divisible only by 7. Dividing the cipher text into seven sections, taking every seventh letter, a frequency count was then taken:

TOP SECRET U.S. EYE

1st 1 6 1 2 1 1 5 1 2 1 3 3 2 1
A B C D E F G H I J L M N O P Q R S T U V W X Y Z

2nd 1 5 3 4 1 3 1 1 2 2 1 2 4
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z etc.

All seven alphabets showed a monoalphabetic distribution, strongly indicating standard sequence. This was confirmed when plain E and N were assigned to the two highest-frequency letters in each of the seven alphabets, and the cipher equivalents fixed by these assumptions produced complete plain text:

DDLUACQ
ACHTSTO

SFVINNN
PERHIEL

WERFLAG
TENURE

QBGIURE
NACARIC etc.

Inspection revealed that the cipher components were displaced from the plain components as follows:

1st - 3
2nd - 1
3rd - 4
4th - 1
5th - 5
6th - 9
7th - 2

Since the series 3-1-4-1-5-9-2 is the numerical equivalent of π , this circuit was dubbed "the pie circuit".

It was later discovered that the traffic from Rio went to Brussels, an auxiliary station for Hamburg.

TOP SECRET ULTRA

2. POLYALPHABETIC SUBSTITUTION-PERIODIC

B. 6-A SHANGHAI-CANTON

A number of clandestine circuits operated in occupied China during 1944 and 1945. The known links of this network were Shanghai and Berlin, Shanghai and Canton, Shanghai and Peking, and Canton and Berlin. The foregoing circuits were designated by the Coast Guard Unit as 6-A, 6-B, 6-C and 6-D, the classification being determined by the class of traffic and systems used. As was the case in South America, portions of this traffic were transmitted over commercial channels, under foreign office cover, as "Auswaertig" or "Diplomata" traffic. Both external and internal evidence in messages indicated that some of it was courier traffic. The bulk of transmissions however, was via radio with typical clandestine characteristics.

The only traffic which was received consistently by the Coast Guard and read was the Shanghai-Canton Circuit.

Systems employed by these circuits were of varying types of complexity, indicating that the Germans were at one and the same time cautious and foolish. Although some of the traffic was Enigma, other circuits employed transposition and still others substitution.

Messages on Circuit 6-A were voluminous and were mostly FLUGVERKEHR reports, listing air traffic between China and India. In addition there was general information about U.S. aid to China, U.S. planes and equipment, and information and rumors in China concerning the U.S.S.R. In the messages the Canton agent was designated as CESAR, and the Shanghai station as CHARLOTTE. Although there is reason to believe that a mechanical device was employed to encipher and decipher messages, no knowledge of the device was necessary for either solution or reading of the messages. The system resolved into a 5-alphabet periodic substitution. Eventually the entire series of 24 alphabets was solved, and from that point reading of all messages became purely a cryptographic process.

Each message transmitted showed a first group which was repeated as the final 5-letter group. A secondary indicator was found to be in the date group, transmitted as a 5-figure group at the end of the message. The last digit of this figure group was the only one concerned with the encipherment of the message. Thus two enciphering tables were necessary: the date table and the square of 24 basic alphabets (X and J were omitted). The basic

TOP SECRET ULTRA

alphabets were random-mixed, and unrelated to each other. The series of letters of column 0 constituted the key-letters from which the particular five alphabets were generated, the starting point being designated by the appropriate column in the date table. Thus each alphabet was a self-generating alphabet produced by sliding against itself, at a starting point designated by the indicator.

DATE TABLE

1	2	3	4	5
6	7	8	9	0
18	3	10	13	8
20	15	22	4	5
17	12	23	6	2
16	24	19	1	12
11	21	9	0	7

BASIC ALPHABETS

2 2 2 2 1 1 1 1 1 1 1 1 1 1 1
0 3 2 1 0 9 8 7 6 5 4 3 2 1 0 9 8 7 6 5 4 3 2 1
A J R G Z L U T H N M D E F S K V O Y I W B P C
B S H K V Y J A I F C N U O T P L Z E R G M E D W
C O J P U S F K N Y R I G W V T D H A B E M L Z
D C U F S T L O E Z Y G B V I J M K P W N R A H
E W K I R B A N M O H Y L D Z V G P F U J S C T
F K Z T L P E J B S O C A M W U I Y D H R V N G
G P T N O D H F A V W E I Z K M C U J S Y L R B
H V L E Y Z T W D P A B C J N I R M S F K O G U
I D W U M O C E J T L A H G P Z N R B K S Y V F
J G S W F K P I R L D H Z N B E A T V C O U Y M
K R D S E C B Z T A G N J P H W O V L Y U I F N
L E F C H U V R G K T O S Y D N Z A I J B W M P
M Z E L W R N Y O G B P V C J F T D U A I K H S
N B Y J C F I D K R P L M T U O S J G Z V H W A
O H V M A E G R L U I J K R Y S F W C P T N Z D
P U N Z R H M G F A S V R E A Y J I T D L C O K
R L B H N V S U Z E J T P I C D W F O M A G K Y
S T G D J M R V P C K N Y U E R H N L F A I O
T A M O P J W C U I V F D S R H Y B A N G Z E L
U C A B K I Y P V N N Z T L G C S E W O H F J R
V I C Y T N O L S H Z U A F R E G M E D P B J
W Y O R D A K H C J E S F B N G P L N V Z T U I
Y F P A I G Z S W K U M N H O L B J E R C D T V
Z E I V G A D M Y B F R O N L A U C H T P J S E

TOP SECRET ULTRA

Thus with a message showing the letter indicator GILKY enciphered on the 19th of the month, showing the figure group 01219, the method of encipherment was as follows:

The last digit of the date-group designated the column of figures from the small number table: -13-4-6-1-0.

The starting point of the successive self-generating alphabets was the letter formed by the intersection of the key-letter found in the standard alphabet in the 0-column of the alphabet table and the letter under column 13 for the first alphabet, column 4 for the second, etc. The five deciphering alphabets for this particular message, therefore, would be:

1. GPTNODHFAVWEIZKMCUJSYLRB
EIZKMCUJSYLRGBPTNODHFAVW
2. IDNUMOCEJTLAHGPZNRBKSYVF
SYVFIDNUMOCEJTLAHGPZNRBK
3. LEFCHUVRGKTOSYDNZAIJBWMP
IJBWMPLEFCHUVRGKTOSYDNZA
4. KRDSECBZTAGMJPHWQVLYUIFN
KRDSECBZTAGMJPHWQVLYUIF
5. YFPAIGZSNMUKNHOLBJERCDTV
YFPAIG, etc.

The type of alphabet square used by this circuit has been designated by the British as a Latin square, as distinguished from a Vigenere square, wherein the alphabets are successively generated from the same basic alphabet.

TOP SECRET ULTRA

C. NONPERIODIC SUBSTITUTION: RUNNING KEY

Chronologically, running-key cipher systems appeared in the Western Hemisphere subsequent to the wide use by Nazi espionage agents of single transposition ciphers, (treated later in this history, all of which ceased with the Brazilian spy roundup in early March, 1942. The testimony of the arrested agents enabled us to find out what books had been employed in the circuits (although all the systems had been read 100% without the benefit of the books). By this time it had become obvious that the Hamburg group had a common transmission style copied from amateur procedure that set it apart from other types on the air, as well as a more or less common cipher system, which once broken in one circuit would give a very good clue to the others in use at the same time. It was also believed that with the public revelation of the ciphers employed in both North and South America, Hamburg would certainly effect some immediate changes, and this proved to be the case.

1. J-G HAMBURG-VALPARAISO

In March, 1942 two new circuits were found which had all the characteristics of the Hamburg group: daily changing calls, slow transmission speed, and voluminous "amateur" chatter. Frequency tables made on the first few messages showed a distribution that was almost random. This fact clearly eliminated transposition as a system. Further tests for repeats gave none other than those which would be expected by random within any single message regardless of length. This indicated a system which either had a very long period or had no period at all. The first four groups were found to contain a concealed enciphered preamble of the usual type, but the function of the fifth group could not be determined. In each case the fifth group contained the same letter three times at varying positions within the group, i.e.,

F G F F Q

S C S S S

V V V R Z

TOP SECRET ULTRA

When some of the enciphered preambles were solved, it was observed that they were derived from sections of Spanish plain text; for example, the first preamble key (Zanischuessel)* solved was:

1 2 3 4 5 6 7 8 9 Ø
E L A V I O N . Ø .

This indicated that a book was probably being used for deriving the keys. Although no repeats of any consequence were found within any one message, it was noted that when the messages enciphered on the same day were written out, and lined up one under the other, repeated trigraphs, digraphs, and single letter repeats showed up between messages, always in the same relative cipher positions.

Message 1. L K N L S W K D T E H X S N L R C L U D I P H E G
" 2. T D E J Z Z F G Y W Y W M T X U Y J F L G O R A A
" 3. I H E P H J F S Y I F C P E A N M S D Y X E R R T
" 4. Y P O P H X P U D H L A S K E U T T K E L E D T
" 5. N K N C F B S R J I (Remainder missing)

Message 1. C Z O Q J T R G F K X Z I E H T R H H U I B Y G H
" 2. M N S S B D V W Y H X Z D V B G G H H F X S H R J
" 3. S D W N R W U S U N V X H M X M M B Q L F R Y V W
4. J C X S A G I N X U F M U Y P R C B P S D V U B C

These repeats, when tested statistically, satisfied the criterion for messages enciphered in the same key. All the phenomena suggested the theory of a running-key system: i.e., one in which the juxtaposition of two sliding alphabets is determined by a continuous aperiodic key, usually taken from a book or magazine. Since the Germans were prone to equip their agents with systems in which the elements could be memorized except for an innocent appearing book, it was hoped, if a running-key had been used, that either straight or reversed normal alphabets had been employed for the sliding alphabets. Acting on this assumption it was decided to try it on the messages already lined up in depth.

The cipher letters in the first position in each message were written out and the plain component completed, likewise the next four or five columns of cipher letters. (See Figure 1)

* ZANISCHUESSEL was the term given to any key providing letter equivalents for the numbers 1 to Ø. A figure may have more than one letter equivalent, but no letter has more than one figure equivalent.

TOP SECRET BULW

Then the lines (or generatrices) which showed the highest percentage of high frequency letters were underlined. (See Figure 1). It was noted that there were two or three lines at least which were possible in each block. By trying all of the possible generatrices in the first block against all possible ones in the second block the two which gave the best digraphs were chosen. The last line of the completed plain component was chosen in column 1 (Figure 1) as the best for beginning the message and the best generatrix in column 2 added to it.

FIGURE 1

Cipher Text	Col. 1	Col. 2	Col. 3	Col. 4
	<u>L T I Y N</u>	<u>K D Y P K</u>	<u>N E E O N</u>	<u>L J P P C</u>
	M U J Z O	L E Z Q L	O F F P O	M K Q Q D
	N V K A P	M P A R M	P G G Q P	N L R R E
	O W L H Q	N G B S N	Q H H R Q	O M S S F
	P X M C R	O H C T O	R I I S R	P N T T G
	Q Y N D S	P I D U P	S J J T S	Q O U J H
	R Z O E T	Q J E V Q	T K K U T	R P V V I
	S A P F U	R K F N R	U L L V U	S Q W W J
	T B Q G V	S L G X S	V M M W V	T R X X K
	U C R H W	T M H Y T	W N N X W	U S Y Y L
	V D S I X	U N I Z U	X O O Y X	V T Z Z M
	W E T J Y	V O J A V	Y P P Z Y	W U A A N
	X F U K Z	W P K B W	Z Q Q A Z	X V B B O
	Y G V L A	X Q L C X	A R R B A	Y W C C P
	Z H W M B	Y R M D Y	B S S C B	Z X D D Q
	<u>A I X N C</u>	<u>Z S N E Z</u>	<u>C T T D C</u>	<u>A Y E E R</u>
	B J Y O D	A T O F A	D U U E D	B Z F F S
	C K Z P E	B U P G B	E V V F E	C A G G T
	D L A Q F	C V Q H C	F W W G F	D B H H U
	E M B R G	D W R I D	G X X H G	E C I I V
	F N C S H	E X S J E	H Y Y I H	F D J J W
	G O D T I	F Y T K F	I Z Z J I	G E K K X
	H P E U J	G Z U L G	J A A K J	H F L L Y
	I Q F V K	H A V M H	K B B L K	I G M M Z
	J R G W L	I B W N I	L C C M L	J H N N A
	K S H X M	J C X O J	M D D N M	K I O O B

Plain Component

TOP SECRET ULTRA

The generatrices chosen from columns 1 and 2 were:

1 2
K A
S T
H O
X F
M A

The digraph XF suggested the familiar X FORTS X used by the Germans in previously solved systems to designate continuations of messages. After having taken the proper generatrices in the next columns to complete this word the other messages read as follows:

1 2 3 4 5 6 7
K A N N E R S
S T E I L U N
H O E R T E N
X F O R T S X
M A N E R W A

With this much plain text as a start, it was not difficult to continue this process until some of the messages were complete. However, when an attempt was made to recover the key by taking the various letters opposite A in the enciphering alphabets through the message, no intelligible text resulted. The same thing was true when the letters in the enciphering alphabet opposite A in the deciphering alphabet were taken. After some study, it was established that the letter of the alphabet whose position in the normal alphabet corresponded to the date of encipherment of the messages was used as a "reference letter", (i.e., on the 1st day A would be used; on the 26th day Z; on the 27th the numbering started over again and A was used; on the 28th B, etc.). This was the letter that appeared three times in the fifth group of the messages in most (out not all) of the circuits using the running-key method. The reference letter was marked on the cipher alphabet which was slid against the plain alphabet -- both alphabets being the standard normal alphabet. The reference letter was set under the key letter and the cipher letter then appeared under the plain text letter.

Taking the cipher text of message 1 in our example above,

L K N L S W K D

and the plain text recovered

K A N N E R S T

the running-key letter can be determined by setting the cipher text under the plain letter and reading the letter opposite the reference letter. Thus,

Plain: P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Cipher: Q R S T U V W X Y Z A B C D E F G H I J K L M N O P

L is set under K; S is the reference letter, (repeated three times in the fifth group); reading above S is R for the running key. This is continued throughout the message as follows:

Key: R I S U E N A S
Plain: K A N N E R S T
Cipher: L K N L S W K D

One result of this procedure was that when the key letter was the same as the plain text letter the resulting cipher letter was the reference letter. Thus,

Cipher: I H S P H J F S Y
Plain: H O E R T E S I

Reference letter - S

Plain: P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Cipher: P Q R S T U V W X Y Z A B C D E F G H I J K L M N O

Key: R I S U E N A S
Plain: H O E R T E S I
Cipher: I H S P H J F S Y

Even though the key and the plain text might be in different languages, certain letters would be high in frequency in both, and consequently the reference letter tended to show higher than random in a frequency count of the cipher text. This proved

TOP SECRET ULTRA

useful in some of the circuits which did not give the reference letter in the fifth group. I.B.A. runs were devised for trying a probable word in the key or plain text through the messages, and for testing generatrices of traffic in depth according to weighted values.

Although there was already another station in operation between Chile and Hamburg, Circuit 3-G was set up as a completely separate unit after the Brazilian spy roundup. Circuit 3-G reported much the same type of information as the former one, giving data on United States equipment and ship movements. It was later learned that 3-G used the Spanish book "SONAR LA VIDA", but this book was not in the possession of this office during the operation of this circuit.

- The solution of Circuit 3-G indicated the type of system which Hamburg would probably employ next. This proved to be true, for the circuits found for a long period after March, 1942 all fell into this category.

2. 4-F HAMBURG-LISBON

The second circuit which was read with the running key substitution method was first intercepted in March, 1942. This circuit used the concealed type preamble located in the first four groups, with the fifth group of cipher text containing the reference letter. The book used for the running key was finally identified as the Portuguese novel "O SERVO DE DEUS." A copy of the book was eventually obtained by this office, which made decryption thereafter purely cryptographic while this type system was being used. The information passed on this circuit concerned movements of Allied vessels from and to Lisbon together with the customary contacts of agents. This circuit had another unusual aspect. Up to this period, the transmission of messages was relatively a simple operation technically. A definite hour was decided upon for a fixed schedule -- weekly, semi-weekly, daily -- and one frequency was allotted to the control station in Hamburg while another was given to the answer. Circuit 4-F at first used only one frequency and one schedule time, but gradually more and more frequencies were given to the answer station in conjunction with more schedule times. This made interception much more difficult than it had been. The frequencies used were usually under some much stronger legitimate station and low power was intentionally used. The Lisbon end of Circuit 4-F was assigned as

TOP SECRET ULTRA

many as eight different frequencies; later on a different set of schedules was issued every week further to camouflage the transmissions.

3. 3-J HAMBURG-SOUTH AMERICA

During May, 1942, a station was found transmitting two messages over again and again for some time. For a few months this station sent what appeared to be about seven different encipherments of the same two messages. The cipher text contained an enciphered preamble in the first four groups. The two messages yielded to solution in the running key method, but the approach was through the different encipherment of the same messages. The text was found to be in German, the running key in Portuguese. It was another attempt by Hamburg to begin operation again in South America, but no contact was ever made with the answer station; after a few months of persistent calling, transmissions ceased.

4. 5-D HAMBURG-THE CRIMEA

Beginning in June, 1942, calls and spotty traffic were received from a station which indicated classification in the Hamburg group. After tests were made, it was found to use the running key method, both the text and key in German, the key derived from an unknown German book. The preamble was enciphered in the first four groups, the fifth group containing the reference letter. The information sent on this circuit was mostly concerned with granting leave to personnel and other administrative matters. Traffic on this circuit was very irregular.

TOP SECRET ULTRA

2. JAMES DOWNINGTON: CHAIRMAN

a. NINETEEN SIXTY

1. 2-5 NINETEEN-NEW YORK

In January, 1941, a suspicious station was heard which used the constant call VVV TEST and which showed the same operating characteristics and type of preamble as the station intercepted the previous October. (See 2-1a). In a short time it was found that there were two other stations in the circuit. A station using the constant call AOR was found to be the control station of VVV TEST, the latter in turn relaying traffic from still another station named GLENN. The traffic sent between AOR and VVV TEST was in five-letter groups with the preamble of two four-letter groups and two three-letter groups. The relay traffic from GLENN to VVV TEST was transmitted with only a letter count and the preamble JSP FOR HENRY or JSP FOR GLENN, depending upon the direction of the traffic.

The same month the Director of the Federal Bureau of Investigation requested the Commandant of the Coast Guard for assistance in the solution of a series of suspicious messages. Upon examination, some of these messages were found to be identical with those transmitted to VVV TEST from GLENN for relay to AOR.

The traffic transmitted between VVV TEST and AOR was examined, and found to have a plain text frequency clearly indicating transposition. Simple columnar transposition was assumed, and attempts made to anagram the columns resulting from assumptions for different key lengths. On one day, among several messages transmitted, one was observed to have a total of 200 letters, another of 400 letters. When these two messages were written out with a twenty-letter key length, certain phenomena were noted:

TOP SECRET ULTRA

Message 1

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	(A)	(C)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)
2	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)
3	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)
4	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)
5	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)
6	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)
7	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)
8	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)
9	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)
10	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)
11	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)
12	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)
13	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)
14	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)
15	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)
16	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)
17	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)
18	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)
19	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)
20	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)

Message 2

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	(A)	(C)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)
2	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)	(H)
3	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)
4	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)
5	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)	(U)
6	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)
7	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)	(D)
8	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)
9	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)
10	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)
11	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)	(A)
12	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)
13	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)
14	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)	(R)
15	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)
16	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)	(P)
17	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)	(T)
18	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)	(E)
19	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)	(S)
20	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)	(L)

- (1) When Message 1 was compared with the ten top lines of Message 2, many letters, including many low-frequency ones, were noted to be in the same position in the same column (see above). Such repeats were not observed by comparing Message 1 with the lower ten lines of Message 2.

TOP SECRET ULTRA

- (2) It was also observed that on line 5 in both messages, the letters H .. I .. K .. J appear, while on line 6 directly underneath them the letters L .. M .. O .. N appear. This led to the consideration that the low-frequency letters seen in both messages could well be nulls inserted into the plain text.

Anagramming was then attempted, and column 4 and 5 were found to produce plausible digraphic combinations for German. These columns gave better digraphs in the second message than in the first, but this assumption was not discarded because of the Q T combinations, for the single letter Q had been used in Circuit 4-A to replace the digraph CH. Thus:

Message 1

4 5
D O
Q T
Q T
T A
I E
M E
T F
Q E
X U
I V

Message 2

4 5
I B
I N
F A
L A
T I
V I
E L
X L
X E
W C
X S
F G
S S
I I
S T
T E
G N
I I
W E
E E



Then, for the German numeral Z40 on line 10 of Message 2 where we already have the letters 40, the only Z on line 10 is in column 9. Adding column 9 to both alignments:

TOP SECRET ULTRA

Message 1

9	4	5
X	T	O
E	I	T
I	Q	T
F	T	A
D	E	E
Q	M	E
E	T	F
O	Q	E
L	X	U
E	I	V

Message 2

9	4	5
E	I	B
E	I	N
B	F	A
E	L	A
L	M	L
E	M	I
X	E	I
N	X	L
Q	X	E
Z	W	O
T	X	S
U	N	G
E	S	S
A	L	L
E	E	G
L	I	E
N	G	X
N	I	Q
Q	W	E
E	R	E

Conceding that I and M are nulls in column 4, all trigraphs seem possible. Continuing the anagramming by assuming the numeral EINS on line 7 of Message 2:

Message 1

9	4	5	14
X	S	O	R
E	Q	T	I
I	Q	T	I
F	T	A	B
D	E	R	
Q	M	E	X
E	T	F	U
O	Q	E	I
L	X	U	N
E	I	V	C

Message 2

9	4	5	14
E	I	B	T
E	I	N	E
B	F	A	H
E	L	A	D
L	M	L	X
E	M	I	N
X	E	I	N
N	X	L	A
Q	X	E	N
Z	W	O	X
T	X	S	Q
U	N	G	S
E	S	S	Q
A	L	L	E
E	E	G	S

etc.

TOP SECRET ULTRA

Anagramming was continued by this method; when a column would fit except for a few letters, by checking each message against the other, the letters which were inconsistent were found to be the assumed nulls.

Message 1.

1	19	16	12	13	7	6	8	9	4	5	14	10	17	2	18	3	20	11	16
(A)D	S	Q	W	E	D	X	D	X	D	O	R	O	T	H	E	A	L	A	(S)
H	E	T	V	E	R	D	A	X	Q	T	I	G	X	C	E	N	G	T	(E)
R	E	M	A	I	U	N	W	I	Q	T	I	G	A	C	M	A	T	Z	(W)
(H)E	E	I	E	E	E	N	O	E	T	T	E	R	(J)I	I	N	S	Z	(K)W	
J	E	I	X	L	I	E	E	E	E	X	D	N	X	X	K	Z	(O)R	(C)S	
E	C	N	A	L	A	D	E	E	T	F	U	E	G	R	I	F	I	E	(S)
F	U	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	(V)

Message 2.

(A)F	I	N	K	S	Q	R	E	I	9	T	F	C	L	L	X	D	X	(D)	
D	E	F	O	W	A	R	E	I	N	E	H	W	C	I	E	H	N	(E)	
R	U	M	E	R	H	A	E	F	A	L	D	Z	E	X	T	N	G	(E)	
(H)T	K	X	E	I	(D)H	G	I	(I)I	L	L	X	(J)X	(C)X	(G)X	A	N	K	(P)	
(I)O	I	A	D	E	T	X	E	(M)I	N	H	(N)O	V	(Q)O	L	E	R	A	(O)A	
S	S	X	N	C	(P)O	A	X	E	I	N	S	D	(R)T	I	G	R	A	(S)P	
(U)S	E	A	N	S	R	I	C	Z	W	O	S	C	F	(T)R	K	S	T	(V)E	
(H)I	N	X	L	A	D	E	T	X	S	(J)F	U	F	(Y)F	E	H	I	E	(X)R	
E	M	E	Z	A	T	Z	U	S	G	F	U	F	(Y)F	E	H	I	E	(A)I	
(G)E	K	A	F	(B)T	A	L	E	(S)I	G	S	(F)C	A	(C)A	I	T	E	R	(G)I	
(O)A	D	E	N	K	R	I	E	(S)I	G	S	(F)C	A	(C)A	I	T	E	R	(G)I	
(H)A	N	G	X	A	L	L	E	(I)E	C	D	T	(J)H	(K)H	E	T	B	R	(O)T	
A	I	E	A	I	T	I	E	(I)E	C	D	T	(J)H	(K)H	E	T	B	R	(O)T	
R	S	E	E	F	I	C	I	E	A	E	F	U	E	R	U	A	S	(R)R	

TOP SECRET ULTRA

Nulls that were not apparent before recovery of the message were obvious after reading the plain text. It will also be noted that the second five lines of the diagram exactly reflect the null pattern of the first five lines. In Message 2, the reflection appears twice. In addition, the nulls have been inserted into the plain text in alphabetical order, starting over again after 2. Further study of the plain text revealed a concise, telegraphic style, with a high percentage of German words abbreviated. This fact helped later on in further anagramming of messages. The biggest help, however, was the null pattern. It was first believed to be applied by the use of a grid for five lines, then turning the grid over on its back for the next five lines. However, after several more keys were recovered, it was found that the nulls were inserted in the plain text diagram according to the numerical transposition key. For example, with the key

1 - 19 - 15 - 12 - 13 - 7 - 8 etc.

the first null would be placed in column 1, line 1, the next null 19 letters from that, the third null 15 letters from the second, etc. After five lines, the nulls thus inserted are reflected for the next five lines, the process beginning over again on line 11. Knowing this principle, when a message was received which had an incomplete diagram, certain long and short columns could be identified by recognizing the nulls on line 5 and those reflected under them on line 0. For example, with a message of 185 letters, enciphered by a twenty-length key, there would be five columns of ten letters and fifteen columns of nine letters. The message is written into a crown diagram with five lines above the original rectangle because of the five long columns:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
T	R	C	D	A	E	A	T	N	A	R	S	K	D	B	P	T	L	M	T
I	E	R	E	E	A	E	E	U	M	T	A	X	E	N	D	O	E	U	I
N	S	A	O	N	K	E	L	E	M	T	N	H	R	G	B	O	H	N	X
T	R	A	E	A	A	E	A	I	A	U	S	K	R	D	A	E	J	R	S
A	S	A	E	A	T	T	N	A	R	Q	K	X	T	P	W	E	C	A	B
S	R	A	E	A	Q	T	N	R	C	D	M	E	D	F	N	E	N	T	T
I	A	A	E	N	M	E	A	R	U	S	I	E	B	T	N	L	R	A	S
E	A	E	U	E	A	E	E	E	E	S	K	X	R	D	W	I	E	T	S
S	A	A	O	A	A	E	A	A	A	N	K	X	E	N	O	E	H	R	B
A	A	A	E	A	T	T	N	A	R	Q	K	X	E	N	E	E	J	A	T
S	R	A	E	A	Q	T	N	R	U	S	I	E	B	T	N	L	R	A	S

column 6, as well as H in column 18. If these are correct, all

the nulls on lines 5 and 6 have been found. Inspecting further, in column 10 F..M can be found on line 4 and its reflection, and in column 15 G..N can be located. Thus, the tops of these columns can definitely be marked off, and any anagramming with these fixed columns will be correct. Continuing the inspection, in column 8 E..L is observed. Thus, if columns 6, 8, and 10 can be fixed at the top, columns 7 and 9 can also be marked off. Thus:

[illegible]

TOP SECRET ULTRA

With this much of a start, anagramming the complete message becomes quite simple:

16	10	3	19	12	5	1	8	13	17	14	9	10	15	6	11	2	20	7
P	L	A	F	S	A	G	T	X	N	E	H	A	T	A	R	R	I	J
T	I	C	U	M	E	N	T	I	S	T	E	A	N	A	T	D	E	M
S	E	R	A	I	L	E	D	O	C	U	M	A	T	U	E	X	A	
N	D	A	N	K	A	E	N	E	R	E	N	S	E	L	B	E		
M	D	A	T	U	M	S	X	E	R	D	S	U	T	E	S	N	E	
A	Y	O	K	H	E	A	D	Q	U	A	T	L	S	R	S	K		
U	M	M	T	X														

VVV TEST-GLENN RELAY

The traffic which was passed on this circuit was tested for a twenty-length key after the solution of the VVV TEST-AOR traffic, but no results were obtained with this key-length. However, two messages were received which appeared to be in the same key and to have similar beginnings:

Message (A)

Y O X N V G S S T N R Z T Y Z V Z G O O I I S etc.

Message (B)

Y O X E U S X E S S N U F S G E S T X Z F V etc.

These messages were lined up and examined for spread repeats, and sixteen repeats were found. (See Figure 2.) The indicated key length of 16 was then confirmed by dividing the total length of the message by 16, and verifying the column lengths shown in Figure 1. Thus, the spread repeats not only revealed the key length, but also separated the long and short columns. In message (A) all six-letter columns were placed in the tentative diagram, leaving all the five-letter columns to follow:

FIGURE 2.

- (A) Y O X H V G S S T N R T Y Z V Z G O O I S S E Y X S G E
I O X L U E S K E S S H U F S G E S T X Z F V B M F X T O H R T A S M Y A N E X Y T E
- (B) G H E L G E H A T R S V I M E C U I E L E X E O E S O A A E
A Z Z S B Z N L G N N Y X E M N T R N R E C S U S E C I S I E R E E etc.
- (C) Y L T Z D N L F L B I R H N E H E V T C S I F Y G R N N
 etc...

Message A -- Total length 89 letters.

Message B -- Total length 140 letters.

Assuming similar beginnings, the messages were examined for spread repeats. Repeats were found with column length of five and six letters in Message A, a length of eight and nine letters in Message B. By counting the number of such repeats, a key length of sixteen letters was determined for each message. It should be noted that since most of these repeats were 2 or 3 letters long, all necessarily had to include at least 2 letters. Therefore, some possible "garbles" were admitted in locating assumed repeats which were consistent with the columnar division of the cipher text.

TOP SECRET ULTRA

1	2	3	8	9	10	12	14	16	4	5	6	7	11	13	15
Y	S	T	T	E	A	Y	R	F	O	S	O	L	O	L	V
X	S	S	S	U	E	T	N	G	I	Y	E	A	L	C	T
N	N	V	V	I	O	E	R	N	I	X	N	H	H	H	S
V	R	Z	I	E	E	D	H	N	S	S	X	A	R	I	I
Q	Z	O	M	L	E	N	E	N							

Because of the numerous occurrences of many low-frequency letters, the latter were considered for possible nulls in anagramming. Placing columns 9 and 14 together because of the good digraph GH:

9	14
E	R
C	H
U	N
I	E
E	H
L	E

The message was then anagrammed:

1	8	10	2	3	9	14	16	12	11	7	6	13	4	5	15
Y	T	E	S	T	E	R	F	Y	O	L	G	L	O	S	V
O	R	X	S	E	T	Z	U	N	G	T	A	E	G	L	I
N	V	O	N	V	I	E	R	Z	E	N	B	I	C	S	
V	I	E	R	E	H	N	D	R	A	I	S	S	I		
G	M	E	Z	G	L	E	N	N							

As in the VVV TEST-AOR traffic, nulls were inserted into the transposition diagram according to the numerical key. About half the traffic transmitted by the GLENN-VVV TEST circuit was found to read on the key shown in the example. Later the key was reversed:

Direct: A N O D E N S T A O M E R E I S
 1 8 10 2 3 9 14 16 12 11 7 6 13 4 5 15

Reverse: S I E R K M O R T S N E D O N A
 14 5 3 12 6 7 10 13 16 15 8 4 2 11 9 1

TOP SECRET ULTRA

After the circuit had been operating for some time, the key was changed to one of 23 letters, but the new key was transmitted in a message in the old key and no solution was necessary. The 23-length key:

G I T T E R A B L E I T E W I D E R S T A N D

There was another portion of this relay traffic which was in a completely different type of system and is taken up in the detail under Section D-3.

The Coast Guard was later advised that station VVV TEST was located in New York, operating under the control of the Federal Bureau of Investigation; the control station AOR was located in Hamburg. The traffic via relay was from and to Mexico City concerning attempts at setting up a direct connection with Hamburg and Berlin. HENRY in the preamble stood for Hamburg, BOSTON for Berlin.

2. 3-C HAMBURG-VALPARAISO

In April, 1941, the monitors found another circuit which had the same characteristics as the TEST-AOR circuit, except that no outside preamble was employed. This circuit used the constant calls REW and PYL, with the control station sounding very much like AOR in Hamburg. It was found that the preamble which had previously been given outside the cipher text was concealed in the first four groups, the Zahlschlüssel based on:

O S Z I L L A T O R F R E Q U E N Z
1 2 3 4 5 . 6 7 . 8 9 . 0 0 0 . 0 .

Thus, the first four groups, employing this key,

S U N I J O J Z E K O R L D C B N R V W
2 1 0 4 . 1 0 3 0 . 1 8 5 . 0 0 0 . 0 .

This traffic was also found to have a plain text frequency count, and several messages were easily anagrammed and the resulting key length was again found to be 20. The key was constant for a short time, then Hamburg issued instructions to reverse it:

TOP SECRET ULTRA

Direct: O N A U D A M P F S G H I F F A H R T
 5 15 14 1 20 6 2 13 16 7 13 4 10 12 8 9 3 11 17 19
 Reverse: T R H A F F I R C S F P M A E U A N O D
 19 17 10 1 7 8 12 11 4 18 9 16 13 2 5 20 3 14 15 6

For security reasons, Hamburg requested another change in key later on, using both the direct and reversed keys.

Direct: S T N A H L U N G S W I D E R S T A N D
 14 17 12 1 7 9 19 10 6 15 20 8 3 5 13 16 18 2 11 4
 Reverse: D N A T S R E D I W S G H U L H A R T S
 3 10 1 17 14 12 5 4 8 20 15 6 11 19 9 7 2 13 16 18

In June, Hamburg sent instructions in the traffic for using an ordinary novel as a key book. The novel selected was the Albatross edition of "SOUTH LATITUDE". The agent was assigned a secret number, to which was added the sum of the day of the month and the number of the month in which a message was enciphered. The resulting total designated the page from which the Zahlsschlüssel, the transposition key, and the call letters for each station were determined. The first 14 different letters of the first line were used for the Zahlsschlüssel, the last 5 letters being variants for G. The initial letters of the first 20 lines (omitting indentations) were taken in order for the literal transposition key. The daily changing calls were derived from the first and last 3 letters of the last line on the page, read in reverse.

It can be seen that by the nature of the procedure for determining the page number, and so long as the secret number remained constant, only 42 keys were possible; therefore, each key was repeated one day earlier in each succeeding month. The same held true for the Zahlsschlüssel and station calls.

3. 3-A HAMBURG-RIO DE JANEIRO

In May, 1944, another circuit, sending the same type of traffic as the previously encountered, was discovered. Cipher texts were ungrammed to produce plain texts and again, the key length was found to be 20. The messages contained a concealed

TOP SECRET ULTRA

4-group preamble, as in the 3-C traffic. Nulls were used as before, but greater care was taken to make them indistinguishable from the other letters of the cipher text. Whenever a series of messages represented sections of one long plain text message, all sections after the first invariably began with FORTSX. This fact was utilized in the application of the Crown diagram technique to the solution of the majority of this traffic.

The Zahlenschlüssel, transposition key, and call letters for this circuit changed daily; but they did not recur in a monthly cycle as did these elements in the 3-C traffic. However, it was discovered that the keys and calls used in the period from the 17th to the last day of one month were repeated in the period from the 1st to the 15th day of the second month following. This led to the conclusion that, in the use of a key book, the page was determined by adding to the agent's secret number the sum of the date of encipherment and 8 times the number of the month. Since no repetition of keys was noted between successive months, it was assumed that the keys were taken from two different parts of the page, alternating month by month. The key book used was "IN THE MIDST OF LIFE", but it was never available to this office.

4. 3-B HAMBURG-RIO DE JANEIRO

The same month, and approximately the same time as Circuit 3-A was discovered, another sister circuit appeared on the air. This circuit used daily changing calls which built up into a cycle, indicating the use of a book in the manner prescribed in the instructions for Circuit 3-C. A twenty-length key was again found to be employed in this traffic, together with a concealed preamble of 4 groups.

This circuit was particularly active in reporting ship movements in the Atlantic, especially in South American ports. For purposes of simplification in reporting, the agent running the circuit used a simple code for certain cities in South America,

AAA—Arrived Rio de Janeiro
BBB—Departed Rio de Janeiro
CCC—Arrived Buenos Aires
DDD—Departed Buenos Aires, etc.

These letters were placed in the transposition diagram twice, i.e.,

C C C X C C C X FRANK STAR etc.

TOP SECRET ULTRA

Thus, when the cipher text was written out in a crown diagram, it was a simple matter to so group these letters as to effect solution. In the ship reports, which formed the bulk of the traffic from the Rio de Janeiro station, the agent did not use any nulls. The book used by this circuit for the calls and keys was the Albatross edition of "THE STORY OF SAN MICHELE", which was not available to this office while the circuit was in operation.

5. 3-D GERMANY-RIO DE JANEIRO

From June, 1941, when it was first discovered, until September, this circuit used a constant twenty-length key as well as the constant calls GEL and ALD. No preamble was used except a group or letter check. Very often messages were sent in sections of 200 letters, for example:

	1/200	2/200	3/45
or	1/40	2/40	3/45

Sending the messages in completely filled rectangles greatly aided the first solution of the key:

8-1-2-15-6-14-16-11-3-17-10-4-9-18-19-20-12-7-5-13

In September, 1941, this circuit changed over to a different type of transposition, and it was found that the German center receiving the traffic was Berlin. For further details see Section D-3.

6. 3-E BREITEN-RIO DE JANEIRO

This circuit was one of the few exceptions to the almost invariable use of a 20-length key for simple columnar transposition. Since the messages were quite long (more than 10 letters per column, as it developed), it was not difficult to anagram the first ones independently of any assumption for the key length, letting the plain text as anagrammed delimit the columnar length. As a result, the key length developed as 15, and the 4th and 6th groups were left over as "buried" preamble or indicator groups.

As the traffic of this circuit continued, the significance of the 4th and 6th groups became obvious. By means of the Landesschlüssel:

TOP SECRET ULTRA

A I A B N Q O L D B R C
1 2 3 4 5 6 7 8 9 0 0 0

The letters of these 2 groups were successfully deciphered to give the day of the month (2 figures), the time of encipherment (4 figures), a serial number (2 figures), and a key number (2 figures). Thus the indicator groups A N A Q K, E C N N A would indicate:

Day of month	15
Time	1600
Message number	05
Key number	51

The continuing solution of messages of this circuit developed an unusual and highly useful relationship between the various keys. It was discovered that the key, for example, for number 52 would be formed by dropping the first letter from the literal key for key number 51 and adding a new letter at the end. It further developed that there were only 49 such keys (numbered from 11 to 77, omitting all numbers involving 8, 9, or 0) and that the literal keys progressed similarly from 17 to 21, 27 to 31, etc., and from 77 back to 11. Thus it became obvious that all keys were derived from a 49-letter literal key which was written into a square and co-ordinately numbered from 1 to 7. The key numbers thus indicated the starting point from which 15 successive letters were taken to form the individual literal key. Eventually, it was therefore possible to generate (with but few ambiguities) all possible numerical keys from relatively few of the originally recovered keys. (Figure 3).

Although it was never possible to recover the complete literal sequence of 49 letters, it was satisfactorily established that the Zahlsschlüssel constituted the first 12 different letters of the literal sequence for key number 11. From this start, it was therefore possible to derive certain of the following letters in the 49-letter sequence, but not enough were recovered to indicate the nature or derivation of the basic 49-letter sequence.

Mulls were inserted into the plain text according to the numerical key for five lines, then reflected, starting over again on line 11 if necessary. The Zahlsschlüssel was also used to indicate numbers in the plain text. In addition, the mulls themselves conveyed a message. For example, a recovered message:

FIGURE 3. CONT'D

[illegible]

TOP SECRET ULTRA

C X R O D X J A N A U S L N I
 V E P Y S A R T H O S S A R T
 H E Y M I T Y C O T M T O L N
 E O O E R R I R Z I N S S F O
 R B E I T T A I N S A R K N
 E H A H A H N E H A H A Y S A
 M E A F O R N C Y C A K K Y
 T A T R A T U A T R I A Y N I
 E T H M A N E A N R N A J U S
 X A S A A M E D A Y B R I (B T etc.

The nulls spell CONVOY NORTH AB HIER X AB It will also be observed that the letters in the first line X R . D X when substituted with the Zehlschlüssel give X O 9 X etc.

7. 5-C HAMBURG-ALGERIA

During 1941 spotty traffic was intermittently intercepted from this circuit. The circuit used a twenty-length key,

17-9-1-16-12-15-10-13-5-11-6-18-2-20-11-3-4-7-8-19

with the customary preamble concealed in the first four groups of cipher text. The Zehlschlüssel was

J E T Z T G E N T D I E F R A G E W O R T
 1 2 3 4 . 5 . 6 . 7 8 . 9 Ø Ø . . Ø Ø . .

Reception was very spasmodic on this circuit, and as a result very little traffic was received for solution.

8. 4-I HAMBURG-BORDEAUX

Traffic received in this office in the month of June, 1942, was found to be enciphered in a simple transposition system using a sixteen-length key. The preamble was concealed in the first four groups of the cipher text, and an extra group for date check was included as the fifth group. There was a separate key for the fifth group date check. Nulls were inserted in the transposition diagram according to the key in the manner previously described.

9. 4-H HAMBURG-UNKNOWN

In September, 1942, five messages were intercepted from a new station which sounded very much like Hamburg. The

4

TOP SECRET ULTRA

Messages showed a frequency count indicating transposition. The messages were analyzed and found to use the customary 20-length key. The messages were a warning from Hamburg concerning security, but no further traffic was ever intercepted. The first four groups of the cipher text contained the preamble, and the nulls were inserted in the transposition diagram according to the numerical key.

TOP SECRET ULTRA

F. LISBON CENTER

1. 4-7 LISBON-PORTUGUESE GUINEA

In October, 1941, a station using the constant call AX7 and its answer station, using changing calls were intercepted. The calls were found to repeat in a monthly cycle. The traffic sent on this circuit was in five-letter groups with a letter check as a preamble. After the traffic was examined, the tenth group was determined to be the indicator:

A B C D E F G H I J
1 2 3 4 5 6 7 8 9 0

Thus,

A B E A B
1 2 5 1 2

probably indicated that page 125 of some book was to be used for a key. When a frequency count was taken, the cipher text was judged to be Spanish transposition with nulls, indicated by the high frequency of the letters K and W. The first significant phenomenon noted in this traffic was that in practically every message the first cipher letter seemed to be a null, and if the message was of fair length, the 19th letter, the 23rd letter, the 37th, etc. also were apparently nulls. If the message was short the space between these apparent nulls tended to decrease. The pattern showed a tendency to repeat in very long messages after about 130 to 220 letters. This indicated encipherment in blocks of some sort. Two messages were discovered which had the same indicator but were of different lengths; these were written out in columns of ten letters each for twenty columns:

TOP SECRET ULTRA

Message 1

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	K	X	A	U	A	G	N	E	G	T	E	D	E	A	I	N	A	J	K	
2	T	X	A	X	N	T	E	A	T	S	E	X	C	E	A	R	L	N	A	E
3	S	O	W	X	N	C	D	Z	D	S	S	A	L	O	V	N	E	T	E	U
4	A	X	X	X	U	E	C	I	W	S	R	A	X	T	N	W	N	O	O	F
5	X	A	S	E	K	Z	I	W	S	R	A	X	T	N	W	N	O	O	F	
6	M	C	X	R	N	X	E	C	X	I	T	T	X	I	K	E	E	F	F	
7	M	S	G	Z	R	C	X	Q	I	R	T	T	X	I	K	E	E	F	F	
8	I	E	N	X	S	U	D	E	P	A	E	R	R	X	E	E	F	F	A	
9	S	Z	S	S	T	D	R	I	W	X	E	W	N	A	O	S	O	X	Y	
10	C	M	E	X	S	D	E	O	P	Z	M	A	T	A	O	R	N	A	R	

Message 2

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	Z	E	X	C	S	X	C	X	U	T	W	M	D	G	L	P	N	C	O	V
2	I	R	S	E	X	R	E	S	E	T	B	O	L	D	N	V	G	O	E	E
3	M	N	W	A	C	A	A	K	I	D	M	N	J	U	F	T	T	Z	E	N
4	D	N	L	E	U	N	V	S	I	C	O	A	R	T	N	P	X	E	E	G
5	E	A	G	P	W	T	E	A	G	S	X	I	O	N	Z	Z	A	N	X	E
6	L	S	X	D	G	R	I	I	E	N	O	E	I	T	M	X	C	V	A	A
7	O	O	I	K	X	A	R	G	C	I	S	R	O	Y	O	A	K	X	X	T
8	I	E	M	R	C	L	R	X	A	G	X	O	M	X	B	R	A	A	X	E
9	E	X	P	C	X	X	N	U	Y	E	S	K	X	N	E	X	E	E	K	R
10	R	M	S	X	S	D	A	N	U	Z	B	A	D	A	B	R	A	O	O	I

Examining the messages for nulls which were obvious, it was noted that the nulls in the odd columns formed a diagonal downwards, i.e.,

Message 2

1	⊙	E	X	C	S	X	C	X	U	⊙	M	D	G	L	P	N	O	O	V		
2	I	R	S	E	X	R	E	S	E	T	B	O	L	D	N	V	G	O	E	E	
3	M	N	⊙	A	C	A	A	K	I	D	M	N	⊙	U	F	T	T	Z	E	N	
4	D	N	L	E	U	N	V	S	I	C	O	A	R	T	N	P	X	E	E	G	
5	E	A	G	P	⊙	T	E	A	G	S	X	I	O	N	⊙	Z	Z	A	N	X	E
6	L	S	X	D	G	R	I	I	E	N	O	E	I	T	M	X	C	V	A	A	
7	O	O	I	K	X	A	R	G	C	I	S	R	O	Y	O	A	⊙	X	X	T	
8	I	E	M	R	C	L	R	X	A	G	X	O	M	X	B	R	A	A	X	E	
9	E	X	P	C	X	X	N	U	⊙	E	S	K	X	N	E	X	E	E	K	R	
10	R	M	S	X	S	D	A	N	U	Z	B	A	D	A	B	R	A	O	O	I	

while the even columns formed a diagonal upwards, i.e.,

TOP SECRET ULTRA

Message 2

```

1 Z E X C S X C X U T M D G L F M U
2 I R S E X R E T E O L D N V G L E N
3 M H W A C A A T I C O A R T N L E E G
4 D N L E U N V A G S X I O N L A N X E
5 E A G P W T E A G S X I O N L A N X E
6 L S X D G R I I E N O E I T M A C V A A
7 O O I X A R G C I S R A L A B R A A X E
8 I E M R C L R X A G K U L A B R A A X E
9 E P C X X N U Y L S A N E X E E K R
10 R M S X S D A N U L B A D A B R A O O I
  
```

Upon reversing all the even columns, the two diagonals of nulls became very apparent:

Message 1

```

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
1 K M X X X D N O G Z A D A A R N A O I
2 T A S N D E I T X M X A E S R X N A
3 S E Y X N U D E D A E R X E E C F A S
4 A S A U C C Q I R A X O H G T X U E
5 X C S R A I O S I A Z T O E N N O S
6 M A X E N E W X R T X O N A D O U F
7 M X G X R E R I S T L I V T E E A N
8 I O N X S C D F S E O R X E R F A E
9 S X S X T T R A M E S N C O A O L A
10 O X E U S G E E F M K T E O I N X R
  
```

Message 2

```

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
1 M X X S D C N U Z A D A L R N O O I
2 I X S C X X E U E E B L N N X G E E R
3 M E R C L A X I G M O J X F R T A E E
4 D O L U A V G I I O R R V N A X X E T
5 E S G D R E I G N X E O T X A V X A
6 L A X P G I A E S O I I N M C N A E
7 O N I E X N S C C S X O T O P K B X G
8 I N M A C A R A D X N E U B T A X N
9 E R P E X R N S Y T S O X D E V E O K E
10 R E S C S X A X U T B M D G B P A O O V
  
```

This determined the size of the rectangle as twenty letters in width, ten in depth. In the diagram of message 1, it is noted that columns 1 and 2 form very good Spanish or Portuguese digraphs as they stand. Taking these as a start:

TOP SECRET ULTRA

1 2
 C W
 T S
 S J
 A S
 X C
 M A
 M X
 I O
 S X
 O X

Column 14 (from message 1) is then added:

1 2 14
 C M A
 T S A
 S E X
 A S K
 X C O
 M A N
 M X V
 I O X
 S X C
 O X E

The same columns are then tried in message 2:

1 2 14
 C M A
 I V N
 M E Y
 D O Y
 E S T
 L A N
 O N T
 I N U
 E R D
 R E G

Both messages give good trigraphs when anagrammed in this fashion.
 Column 17 is then added on:

TOP SECRET ULTRA

Message 1

	1	1		
	1	2	4	7
K	M	A	N	D
T	A	R		
S	E	X	C	
A	S	T		
X	C	O	N	D
M	A	N	D	
M	X	V		
I	O	X	F	
S	X	C	O	
O	X	E	N	

Message 2

	1	1		
	1	2	4	7
M	A	N	D	
I	O	X	F	
M	E	X	T	
D	O	X		
E	S	T	A	
L	A	N	C	
O	N	T		
I	N	T	A	
E	R	D	E	
R	E	F	A	

The completed rectangles:

Message 1

A	R	K	M	A	N	D	O	X	D	I	Z	X	N	T	A	O	X	G	A
R	S	T	A	R	X	N	A	D	A	X	S	E	M	X	I	N	T	E	
R	E	S	E	X	C	T	A	M	O	S	A	X	D	E	F	E	N	D	E
X	G	A	S	T	O	U	X	C	E	R	C	A	X	I	L	N			
Z	E	X	C	O	N	T	O	S	X	S	I	R	I	A	N	D	K	S	M
X	M	A	N	D	O	U	X	F	R	E	E	T	O	F	N	X	A		
L	E	M	X	V	I	A	G	E	N	S	X	T	E	R	R	I	T		
O	R	I	O	X	F	R	A	N	C	E	S	X	O	E	S	P	E		
S	A	S	X	C	O	N	T	A	V	X	R	E	L	A	T	O			
K	I	O	X	E	N	T	E	R	E	U	E	N	X	S	P	O			

Message 2

A	R	M	A	N	D	O	X	D	I	Z	X	C	O	N	S	O	L		
K	X	I	N	G	L	E	S	X	R	E	C	E	B	Z	U	X	E	N	
O	R	M	E	X	T	E	I	E	G	R	A	M	A	X	C	I	F		
R	A	D	O	X	R	E	L	A	T	K	V	O	X	G	U	I	N		
E	X	E	S	T	A	O	X	G	R	A	N	D	E	X	V	I	G	Z	
I	L	A	N	C	I	A	X	T	E	S	P	I	O	N	A	G	E	M	
X	P	O	N	T	K	O	X	I	N	G	L	E	R	S	E	S	X	C	O
N	T	I	N	U	A	M	"	A	N	D	A	R	X	Z	C	A	B		
O	V	E	R	D	E	X	K	P	R	E	T	E	N	S	O	S	X	V	E
M	P	R	E	G	A	D	O	S	X	V	T	C	A	B	O	X	S	U	R

Both messages had remainders which were enciphered in the same key in a separate block. It was found that long messages were always cut into rectangles each ten letters deep, and each rectangle transposed as an entity. The indicator was found to control, by the first three letters, the page of the book used, and to designate the width of the diagram by the last two letters:

A B E B J

1 2 5/2 0 - 20 length diagram

TOP SECRET ULTRA

Since the width of the rectangle was a constantly changing factor, repeated keys seldom occurred. The use of the nulls, both in the letters themselves and their position, proved to be of great help in reading the traffic.

2. 4-C LISPA-LOURENCO MARQUES

In the same month, October, another circuit displaying many of the same characteristics as 4-B was found. This particular circuit used the constant call U02 and the answer station a series of changing calls in a monthly cycle. After solution of circuit 4-B, the new circuit was examined for the possibility of Portuguese transposition. A frequency count indicated this assumption to be correct. Like 4-B, there was also a high number of the letters K and N, indicating nulls. An indicator was found in the eighth group, the middle three letters of which were always among the first ten letters of the alphabet. This suggested the familiar method of designating a page from a book to be used as a key. Thus,

A B C D E F G H I J
1 2 3 4 5 6 7 8 9 0

Therefore,

X A D B S
. 1 4 2 .

would indicate page 142 to be used. Also the fact that only three letters of the indicator group were significant led to the conclusion that only a page was designated by the indicator group and therefore a constant width was probably employed. A letter check of the cipher text was the only preamble used. In a message of 85 letters, taking out the indicator left a total of 80 letters to be used in the diagram. A key length of twenty letters was attempted at first but no result was obtained. Then different lengths were tried. When a length of sixteen letters was employed a phenomenon appeared which proved that the right key length had been attained.

									1	1	1	1	1	1	1	
									1	2	3	4	5	6	7	8
1	Y	E	O	S	E	R	N	E	Y	R	C	E	X	D	F	O
2	4	Q	A	P	O	F	X	C	A	N	E	E	X	C	S	
3	S	R	Z	N	A	O	X	X	4	Y	A	A	X	L	I	
4	A	O	R	K	M	X	T	M	Q	I	O	Y	A	L	E	O
5	X	O	I	E	N	C	Q	U	E	A	X	Y	M	B	M	

The most obvious nulls fell into diagonals which began on columns 1 and 9. Anagramming was then attempted, starting with the letter Q on line 5, column 7:

7
F
X
O
I
2

Adding column 9.

7	9
N	A
X	A
O	X
I	2
2	U

Ther. column 4,

7	9	4
N	W	S
X	A	P
O	X	N
I	Q	K
U	R	

it was found that good trigraphs resulted. Anagramming was then continued until the message was recovered.

1 1 1 1 1 1
8 0 1 4 2 6 5 1 6 3 5 3 7 9 4 2
E N Y D E R E C O X F O N G S E
C K A X K F O N S E C A X A P E
N A S X N A W Y I A L Z O X N A
M I A L O X M C C A M B I Q K W
U E X M O C W A M J B I Q U E X

However, only in rare instances was a completely filled rectangle sent by this circuit. The diagonal insertion of nulls greatly aided solution in cases of incompletely filled rectangles. For example, in a message of 275 letters, it could be determined that there would be three long columns of 10 letters and thirteen columns of 17 letters because a constant key length of sixteen was always used. The message is written out in a diagram with the three long columns at the left hand side:

12
TOP SECRET ULTRA

```

1 W R E A E N N O X
2 X Z T I I O E I C X U T
3 S S A O E T X I U Q X
4 S A S L T E S C A S N R D A R
5 P E X D I A A U S P V Y L A
6 E N U X D S A A R A N F A T T E
7 T X S A I R A A T M O X X A R
8 O E X A X X U I P X R S C S P
9 G C X A Y W N C R G D A A A
10 V N N K V X S S E C K A Y E E
11 S D C A S A T E N O A I T E
12 I R O E A U D P X C O P R A N O
13 X A N A N A X X T C I T A E I
14 N O P I A O R C O R X M T R V O
15 J S P M T R M C A R E M R X O C
16 K O U E U R C A I X A S X U N
17 O M X

```

The text is then inspected for obvious nulls:

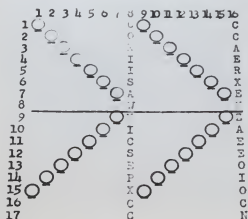
```

1 W R E A E N N O X
2 X Z T I I O E I C X U T
3 S S A O E T X I U Q X
4 S A S L T E S C A S N R D A R
5 P E X D I A A U S P V Y L A
6 E N U X D S A A R A N F A T T E
7 T X S A I R A A T M O X X A R
8 O E X A X X U I P X R S C S P
9 G C X A Y W N C R G D A A A
10 V N N K V X S S E C K A Y E E
11 S D C A S A T E N O A I T E
12 I R O E A U D P X C O P R A N O
13 X A N A N A X X T C I T A E I
14 N O P I A O R C O R X M T R V O
15 J S P M T R M C A R E M R X O C
16 K O U E U R C A I X A S X U N
17 O M X

```

The nulls are found to fit into a definite pattern. Since previous experience demonstrated that the diagram must be 16 columns in width, and that the nulls progressed downwards starting in columns 1 and 9, then progression must be reversed on line 9 starting in columns 8 and 16. Columns 8 and 16 can be placed immediately in their correct position because of the double nulls falling on lines 8 and 9.

TOP SECRET ULTRA



Column 1 must have a null on line 1 and nulls on lines 16 and 17:

- 1 (X)
- 2 X
- 3 S
- 4 X
- 5 S
- 6 P
- 7 E
- 8 T
- 9 O
- 10 G
- 11 V
- 12 S
- 13 I
- 14 X
- 15 N
- 16 (X)
- 17 (X)
- 18 O

Thus, by counting off according to the null pattern, the diagram can be filled and the three long columns found:

TOP SECRET ULTRA

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	Q	R	M	M	U	R	C	O	X	Q	A	I	A	A	I	E	C	
2	X	C	E	X	E	N	N	O	X	Q	A	I	A	A	I	E	C	
3	S	T	A	I	O	E	I	C	X	U	Q	A	I	A	A	I	E	C
4	S	S	A	I	O	E	I	C	X	U	Q	A	I	A	A	I	E	C
5	P	E	T	O	E	T	E	S	C	A	S	N	R	O	X			
6	E	N	X	S	L	A	A	A	A	A	A	A	A	A	A	A	A	A
7	T	X	U	D	I	S	A	A	A	A	A	A	A	A	A	A	A	A
8	O	E	S	I	D	R	A	A	A	A	A	A	A	A	A	A	A	A
9	G	C	X	A	I	X	N	C	R	G	D	R	A	A	A	A	A	A
10	V	N	D	N	A	X	A	S	S	E	C	X	A	A	A	A	A	A
11	S	D	N	A	X	A	S	S	E	C	X	A	A	A	A	A	A	A
12	I	R	C	A	V	A	T	E	N	O	R	A	A	A	A	A	A	A
13	X	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
14	N	I	N	E	A	A	X	X	T	R	C	I	T	R	V	O	C	
15	N	I	N	E	A	A	X	X	T	R	C	I	T	R	V	O	C	
16	O	S	P	A	N	O	R	C	O	R	X	M	T	X	O	C		
17	O	P	I	A	R	M	C	O	R	E	H	R	A	U	N			
18	O																	

By placing the three long columns together,

5 13
 M O A
 E A I
 E S S
 J A J
 R S R
 L P R
 L E V
 I T A
 D O X
 I G O
 X V V
 R S R
 V I I
 S X R
 A N T
 M I T
 A R R
 T O S

good trigraphs are noted. Then by anagramming the remainder, the message is recovered:

5 M E E X X S S E L I D I V S Y A N A T O S
 13 J J A U N T U S A E N X S C G A I A X X X U
 24 I F A D I J A A I C E S T E N E V O C U
 15 C O R S A A A P O S E R A N C O I M P
 12 X X I X X X X X X X X X X X X X X
 30 A A A A A A A A A A A A A A A A A
 4 U X X U L C O S U R A F R A N X T A I
 2 X X X X X X X X X X X X X X X X
 11 C C A E R X E X P E N D A E O I O C N
 7 R N C E X X X X X X X X X X X X X X

TOP SECRET ULTRA

c. STUTTGART CENTER

1. 4-7. STUTTGART-LITVA

In July 1942, a circuit was intercepted which used the constant call F L G for the control, changing calls for the answer station. The traffic sent by this station was prefaced by a letter check for the preamble, and the traffic itself showed a frequency count for German transposition. The control sent a message of 206 letters for several days, and a twenty-length key was tried on the message. The tenth group (AHANE) was selected as being the possible indicator because of the way the letters were arranged in the group as well as the fact that only letters within the first ten of the alphabet were used. The message was written out in a diagram:

1	2	3	4	5	6	7	8	9	0	1	1	1	1	1	1	1	1	2
L	E	A	A	A	L	A	Q	R	L	X	G	T	T	T	X	E	X	N
A	M	T	G	B	L	D	G	T	E	Q	L	B	I	N	T	N	E	U
A	T	L	R	S	R	E	U	T	D	B	F	A	X	B	E	I	E	N
T	F	K	S	S	E	C	Z	A	N	S	L	E	T	E	G	A	N	L
N	X	E	I	O	L	O	Z	E	H	T	Q	M	I	Q	R	R	E	R
F	R	N	U	L	R	X	B	N	F	L	M	H	R	U	U	X	E	E
B	I	E	Z	D	E	N	F	O	T	X	U	R	X	X	X	G	B	X
K	S	R	E	U	S	E	G	M	I	R	D	L	W	O	N	L	N	U
E	I	M	E	X	G	L	G	E	X	O	G	E	X	D	R	S	S	X
Y	I	R	T	H	X	H	N	D	O	L	N	A	E	S	H	R	T	N
U	E	A	A	A	L	A	Q	R	L	X	G	T	T	T	X	E	X	N
L																		

Anagramming was then attempted, noting that columns 14 and 15 form good diagrams:

1 1
4 5
T T
B I
X B
T E
I Q
R U
X X
N O
X D
E S
T T

Column 13 was then added:

T T E
B I N
X B E
T E N
I Q E
R U E
Y X B
W O N
X D S
E S T
T T X

However, no other columns were found to add to this combination. Going back to the cipher text again, it was believed that another group might have been the indicator, but this produced no further results. Writing out the cipher text in columns of five, an unusual phenomenon was noted:

A B L R E N A U A A L A R L Y A B Q etc.
A K M I T E G Z B H D L E D N G F T
T E T S L R R E S A U R S E E U G T
N X F I K M S E S H X E G C L Z G A
F U X I E R I T O E H L X G H Z N E

Reading the letters on a diagonal, it is found that a good German word is spelled out—AKTIENGESELLSCHAFT. Deciding that these letters could very well be nulls inserted in the cipher text, they were not considered as part of the columns for anagramming. Thus, fitting a Z on the combination WO and a G on the combination RUE

O T T E
X B I N
N X E E
E T E N
L I Q E
G R U E
U X X B
Z W O N
Z X D S
B E S T
G T T X

It can be seen that the bottom line anagrammed out is not producing plain text, and that the arbitrary line above (O T T E) from the crown diagram gives a possible plain-text combination. Continuing the anagramming process, the complete message was recovered:

TOP SECRET ULTRA

[illegible]

It was further observed that the letters considered as nulls were actually the literal key for the transposition—AKTIENGESELLSCHAFT:

A K T I E N G E S E L L S C H A F T
 1 1 1 1 1 1 1 1
 1 1 7 0 4 4 8 5 5 6 2 3 6 3 9 2 7 8

The indicator in this particular message

А Н А Н Е
1 8 1 8

contained the length of the transposition key twice, in the first four letters, the fifth letter being part of the literal key. On later messages the literal key was inserted into the cipher text in the same fashion, and it was possible through this knowledge to reduce reading messages to a purely cryptographic process. For example, the key can clearly be seen:

A A T N F B (K) E X U L M (T) F X R I S (I) E T L K (E)
(N) E R M R A (G) R S I U Z (E) E T A P S (S) O A H A H (E)
(L) D U X H A (L) R E L R E (S) G X L D E (C) O X N E L (H) etc.

TOP SECRET ULTRA

D2. SINGLE TRANSPOSITION: COMBS

1. 3-F COLOGNE-RIO DE JANEIRO

Traffic on this circuit was first intercepted in the fall of 1941. Although obviously transposition, it did not have any of the external characteristics of the columnar transposition systems. There was no enciphered preamble or indicator and the usual preamble was only a letter check. The call letters changed daily for each station. As the traffic continued, it became evident that the call itself was an indicator for the date of encipherment which was apparently the controlling element in the selection of whatever key was employed. This was disclosed by the fact that frequently, in the preamble, the letter check was preceded by three letters which were invariably the call letters for the originating station one day or more preceding the date of transmission. Although nulls were apparent in the cipher text, there was no apparent symmetry or homogeneity about them or their position. All attempts to anagram them for single columnar transposition were unavailing.

Eventually, one significant phenomenon became apparent. In cases where a series of messages in the same key could conceivably be successive sections of one long message, it frequently happened that the first letter of each part after the first was an F. It was invariably true that, if one such part started with F all succeeding parts did likewise. There was even a special case of this sort where four such possible continuations all started with FO. This suggested that these were actual continuations and that the usual stereotyped beginning for continuations (i.e., FORTSX) was being used with typical consistency.

In the course of studying the cipher text of individual messages, there often seemed to be at least one case of two segments of cipher text forming very likely digraphic combinations when aligned. These alignments on occasion even seemed to produce reasonable digraphs for a distance disproportionately long with respect to the length of the message. Furthermore, it always remained impossible to expand such alignments into plausible tri-graphic combinations, or even to find two logical digraphic alignments of equal length.

50

TOP SECRET ULTRA

Finally, however, in studying one message in this series, the alignment (although relatively evenly spaced) digraphs were variations which were almost perfect. The resulting digraphs were principally those characteristic of plaintext (i.e., th, sh, ch, ph) for which the letter following could be predicted with reasonable certainty. A sequence of most of the anticipated letters was found in the cipher text, but in reverse order. Such this sequence was inverted and aligned with the first alignment, then the sequence was read off, where an expected letter was absent, that position was skipped and the columns were stretched out. Moreover, when the second and third columns of the alignment were extended beyond the original starting points, more good digraphs were formed; and by judicious stretching of these two the first one could be extended to form good trigrams with the last two. Similarly, a fourth sequence was found which could be prefixed to the alignment of three columns when these were expanded to a greater degree. At this point, there were several numbers completely spelled out, and a revelation of what could be nothing but plain text; the longest column was on the left, the columns became progressively shorter from left to right, and when a line was skipped in one column it remained blank in every column to the right of that point.

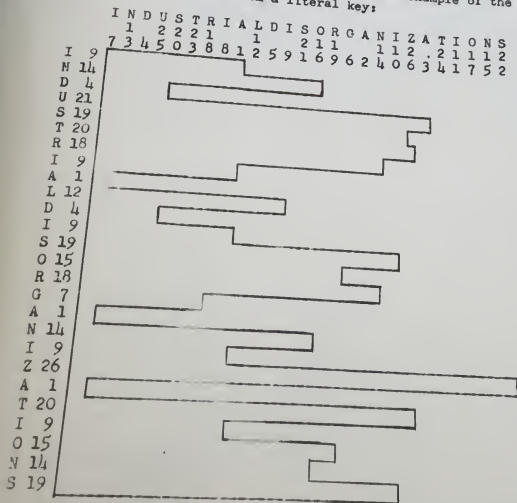
With these criteria, the four successive messages starting with FO were ungrammed in a similar fashion for the beginning with FO and simultaneously expanded into the complete plain text. (The fact that the first section of this message was of the same length as the first continuation facilitated the full recovery of the plain text in no small degree.)

When the plain text was fully recovered for this series of messages, it was discovered that the diagrams in which the messages had been inscribed roughly resembled combs with teeth of irregular length. They were identical for this series from the top down, differing only in the length of the bottom portions as the length of the messages varied. The base of the comb was the left hand margin with the teeth extending irregular distances to the right. The inscription had been horizontal into each tooth in succession. The transcription had been vertical -- sometimes direct and sometimes reversed -- according to the same columnar transposition key for each message in this series. The literal key, from which this numerical key had been derived, was recovered without difficulty and proved to be English -- which was quite evidently the beginning of a verse from the Bible, starting with AND. Furthermore, upon recovery of the literal key, it became obvious that the length of each successive tooth was equal to the number, in the normal alphabet, of each successive letter of the literal key. The

TOP SECRET ULTRA

longest message in this series had 26 teeth, thus enabling the recovery of a 26-letter literal key (the one first recovered had been somewhat shorter, due to no teeth being the maximum length of a Z in the literal key). When a new numerical key was derived from this 26-letter key, it became obvious that this numerical key had controlled the direction of the transcription of the columns (i.e., the odd-numbered columns had been transcribed directly; the even-numbered columns in reverse).

The following diagram will furnish an example of the generation of such a comb from a literal key:



TOP SECRET ULTRA

The message would be inscribed horizontally into the outlined portion of the diagram. Nulls would be used to fill out the remainder of the row in which the message ended and the following one or two rows. Transcription would be downwards for the odd numbered columns and upwards for the even numbered columns.

After solution of one or two other keys, two characteristics became apparent: first that the date determined the page from which the literal key and call letters were taken -- page = 30 x number of months past + day + 10 (1941) + 20 (1942); and second, that the call letters thus indicated the date, being inserted in the preamble to indicate a date of encipherment different from the date of transmission. The literal key was the first 26 letters on the page, from which the numerical key was derived and the Comb generated. In transcribing the columns, the odd numbered ones were taken in direct order, the even numbered ones in reverse order. It should be noted that, by the conventions of the system, 26 letters had to be taken in order to provide a 26 width column key. Since one of the letters might be Z, the maximum length of any row was fixed as 26. Similarly, since the maximum length of the literal key was 26, the maximum capacity of any diagram was 26 rows. Even though no row happened to extend the full width of the diagram, nevertheless a 26-number key was first derived and the numbers from the key controlled the direction of the transcription.

From the mechanics of the system, it can be seen that, if the first letter of the key were an A, the first number of the columnar key would be 1, the first row would contain only one letter, and the second letter of the plain text would fall at the beginning of the second row, i.e., in column 1 of the columnar key -- so that the first 2 letters of the plain text would become the first 2 letters of the cipher text. This fact was of considerable help in reading the majority of this traffic without the correct edition of the Bible--since, as in the case of the FO series of messages, every time the word AND was first on a page, the first 2 letters of the cipher text would provide a start on anagramming the plain text. Just previous to the closing up of this circuit the British provided us with the correct edition and all the traffic was read. The correct edition proved to be the "Bluejacket" edition of the King James Version of the Bible, issued to all British servicemen.

2. 3-H HAMBURG-SAO PAULO

In August, 1941, the control station of this circuit, which was the only side of the circuit heard, was intercepted using the constant

53
TOP SECRET ULTRA

call MIT. The volume of traffic received on this circuit was slight, and the frequency count taken on the traffic showed that a transposition cipher was employed. Trial was made on the German favorite twenty-length key, but this gave no result, nor did other length keys. The theory then was advanced that the system utilized might be of the comb type. After a considerable number of trials, five messages were read in a comb system, a different key being used for each day, leading to the assumption that a book was employed for the keys. In July, 1943, after apprehension of the agent involved in this case, it was discovered that when the circuit was originally started the constant phrase INCONSTITUCION ALIENAMENTE was used for the key. Then after contact was established, the agent was instructed to use the book "PAGEL IN GINECK" for extracting the key, which was always the first 26 letters of the page of the day. The page of the day was established by a somewhat different scheme than the regular Hamburg method: the agent's number (in this case 20) was added to the day of the year. For example, if the date were February 15, which is the 46th day of the year, the page of the book to be used would equal to 46 plus 20, or 66. The agent was further instructed that when this method could no longer be used, due to the size of the number being greater than the number of pages in the book, a new system would be instituted. When the agent was actually apprehended, he handed over a copy of "THE MARTYRDOM OF MAN" to the investigators. None of these books were available to this office.

3. 4-E. HAMBURG-LISBON

The traffic on this circuit was at first thought to be simple columnar transposition, since it employed the customary four group buried preamble. After the solution of the 3-F circuit, however, this traffic was also discovered to use the Comb transposition. Only 6 keys were recovered for this traffic. The fifth group of the cipher text proved to be either a dummy group or an indicator for the date of encipherment. The book was either Spanish or Portuguese and the page was apparently chosen by the formula: 17 times the month plus the day of the month plus the agent's number. The literal key was apparently composed of the initial letters of successive lines, but in some fashion, each time the same page was used, the key was started at a point farther down the page.

TOP SECRET ULTRA

D3. SINGLE TRANSPOSITION: BRILLES

1. BRAJOB-VOLCO CIRCUIT BERLIN-MEXICO
AND 2-B BERLIN-MEXICO

Late in the fall of 1940, the monitors who were covering the commercial circuit from Chapultepec, Mexico to Muen, Germany at the request of the F.B.I., intercepted some five-letter traffic emanating from Mexico City to Berlin which appeared suspicious. This particular traffic was sent from the cable address VOLCO in Mexico City to the address BRAJOB in Berlin, and it displayed characteristics of a cipher system instead of the customary code or enciphered code types usually found in commercial circuits. Examination revealed the messages to be in a system which was obviously transposition, and the frequency count indicated that the language employed was German, using low frequency letters as nulls. After some study the third group of each message was spotted as an indicator. The first three letters of this group were within the first ten letters of the alphabet, and there were only four different letters used as a fifth letter of the group; the fourth letter was random and appeared to be a null.

i.e., ABGZD
ADBVD
CJCRF

Another curious fact also became evident. When the message, exclusive of the indicator group, was not 135 letters or a multiple of 135, there was always a number inserted in the message. This number, it was found, came after a number of letters which was a multiple of 135, and it was equal to the number of letters following it in the message. For example, in a message of 111 groups (or 555 letters), the number 15 would appear after the 108th group. This suggested some sort of encipherment by blocks of 135 letters. The fact that only four letters were used in the fifth position of the indicator suggested a four-cornered diagram. Acting on this theory, a message which contained 441 letters was lined up in lengths of 135 letters, i.e.,

1	135
136	270
271	405

omitting the indicator in the third group, and leaving a remainder of 36 letters.

TOP SECRET ULTRA

¹₅ E A W I Z T X I M A U J X F A R S D U X B X T I E X S U S U
¹₅ I E U R Y R T X V E A Z H E E B O O O I N Z D N N N T N E V
²₅ U I U H Z F G E C E E Z E N L U X W F K C T X B R E D N I N

³₅ L X N C L N Z N X O A E E U J B E U E L U F E V I L C N A I
⁴₅ F N A B H C X F E H E A D R J X U E I I T G A L P A N Z U N
⁵₅ M F O L A B E N N X R R W R Y X E L H L W F E E O E T A I L

⁶₅ N X L B T N L N Y E D L Z S W T X S F Y L O Z N I N N N X X
⁷₅ S Z M D I M N X Y O N E J H K U N V W J I F Z O I R E N S R
⁸₅ L R T A E N O U J R R X J E N E X X U O O S J N I C E R U V

⁹₅ U H L E L U S U Y E X M A F X I A C L S R X D N H N X R Z
¹₅ I I U N D F X L C Y E F E R F T I X T E I E R N L D E R R R
¹₅ E D I B A X V U E Z A H H Z Z M V L A U V X A I U G A Z I G

¹₅ Y M R X U H N X I L I J I N Z
¹₃ Z E X N X X I R I L O Z Z E E
¹₅ Y M S T N A O N B W S Z S D T

TOP SECRET ULTRA

Since nothing at all was known about the possible subject matter of the message to provide an entering wedge, it was thought best at first to try anagramming for German numbers. Of the ten German numbers ZWO was chosen as the best to work with, because it involved two of the most infrequent letters, thus necessitating fewer trials. In such a case it was necessary to try all combinations of the letters Z, W, and O in each block to see if good tri-graphs would result. Taking columns 37, 3, and 40,

37 3 40
Z W O
X U H
E U X

the tri-graph EUX was discarded as being unlikely. However, the combination of columns 37, 75, and 40 gave good tri-graphs:

37 75 40
Z W O
X K H
E N X

The tri-graph X K H was not discarded because the German abbreviation KHZ (for Kiloherz (kilocycle)) had been previously encountered. Then by adding column 58,

37 75 40 58
Z W O N
X K H Z
E N X A

the German numbers NULL or NEUN were suggested. NULL proved to be correct, as shown hereafter. In the process of anagramming, certain columns were not used because of the obvious use of low frequency letters leading to the assumption that they constituted nulls:

5 12 45 69 73 etc.
Z J J Y Z
Y Z J Y J
Z Z Y J J

Some columns could be fitted, but no completely satisfactory arrangement resulted. It was then found necessary to leave many blank spaces for fitting. Only by the following placement could the actual progression of the columns be maintained:

```
38 xx 123 39 1 60 xxx 61 78 20 xx 103 104
xx 77 122 xx xx 59 124 62 79 xx 19 xxx 105
```

By continuing the placement of the other columns of the message, it was noted that some of the columns progressed upward, others downward:

```
123      104
122      105
121      xxx
106      etc.
```

The continual process of adding to these columns, and at the same time anagramming for plain text, brought about completion of the message, as shown on the following page. A tentative diagram was then developed:

```
  4  8 12 5 1 6 13 7 9 3 2 10 11
38 xx 123 39 1 60 xxx 61 78 20 xx 103 104
xx 77 122 xx xx 59 124 62 79 xx 19 xxx 105
xx 76 121 xx 2 xx xxx xx 80 21 xx 102 xxx
37 75 xxx 40 xx 58 125 63 81 xx xx xxx 106
xx xx 120 xx 3 xx xxx xx 82 22 xx 101 107
36 74 xxx 41 xx 57 126 xx xx 23 18 100 xxx etc.
```

This diagram could not be made accurate from a single message, because it was impossible to place correctly most of the nulls. It was uncertain into which column certain numbers at the beginnings or endings of columns should be placed, and in addition, whole columns could be interchanged.

When a second message was anagrammed with the aid of the tentative diagram, most of the ambiguity was straightened out, because the use of a different key determined the beginnings and endings of all the columns more accurately. Later another message was anagrammed in which the diagram proved to be a mirror image of the one previously used. This determined conclusively that some type of overlay with two faces was being employed; this also enabled the null cells to be accurately placed, since the null apertures on one face were not necessarily designated for nulls on the other face. (See Figure 5).

TOP SECRET ULTRA

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
3	2	3	2	1	6	6	7	2	1	1	1	2	2	5	2	6	7	1	1
N	R	X	X	E	I	N	S	X	M	A	X	M	A	X	X	F	U	F	U
F	S	N	U	L	L	S	V	I	E	R	N	E	U	I	Z	W	O	F	Z

3	7	4	5	1	6	8	1	1	8	2	2	1	1	3	7	4	5	1	2
Z	W	O	N	U	L	L	X	Z	W	O	X	E	I	C	S	A	C	H	T
X	K	H	Z	X	N	T	M	R	U	F	Z	A	V	B	E	R	A	X	I

4	2	4	1	2	9	9	5	5	1	2	8	1	4	5	8	9	1	3	7
E	I	N	U	L	L	X	B	I	S	O	X	Z	E	D	W	O	N	L	C
R	H	O	E	A	N	A	A	N	B	X	R	Z	P	O	N	U	L	L	X

1	1	4	3	8	2	9	3	7	1	7	5	3	1	8	2	1	5	9	1
6	7	4	0	5	6	7	3	1	7	7	5	3	1	8	2	1	5	9	1
B	E	R	L	I	N	X	N	D	X	T	E	O	S	C	D	L	A	G	E

5	8	2	9	1	3	4	1	3	2	1	9	6	1	1	4	5	1	3	8
2	7	8	5	0	2	6	3	3	9	3	4	8	6	1	1	4	5	1	3
F	N	U	L	L	X	B	I	S	X	E	I	N	S	D	E	U	N	N	U

6	4	5	6	8	3	9	1	1	4	3	9	1	9	1	4	5	1	3	8
3	5	0	7	9	0	2	2	3	9	9	5	0	0	1	4	5	1	3	8
N	U	L	L	N	U	H	R	X	M	E	Z	X	A	U	L	L	O	R	N

Columns 5, 12, 45, 70, 75, 80, 100, 121, and 132 are nulls.

TOP SECRET ULTRA

FIGURE 5

D

	4	8	12	5	1	6	13	7	9	3	2	10	11	- Key
38	X	123	37	1	60	X	61	78	20	X	103	104		
X	77	22	X		59	124	62	79		19	X	105		
X	76	21	X	2			X	60	21		102			
37	75		40		58	125	63	81				106		
X		120		3				82	22		101	107		
36	74		41		57	126			23	18	100			
X		119	42	4		127		83			99			
35	73				56	128	64		24	17				
X		118	43	5	55			84			98	108		
34	72			6	54	129			25	16				
X		117	44			130		85	26		97			
33	71			7	53	131		86	27	15		109		
X		116				132	65			14	96			
X	70	115	45		52			87	28		95	110		
32			46			133			29	13	94			
X	69			8			66			12		111		
X		114	47		51	134		88		11	93			
31	68		48		50		67	89	30		92	112		
X		113		9	49	135		90		10	91			

The overlay proved to be a rectangle of 13 by 19 cells, with only 135 of the cells cut out. In the process of enciphering a message, this grille was placed on a piece of cross-section paper and the message was written out from left to right in the normal manner through the cut-out cells (except that some of these cut-out cells were specially marked for the insertion of nulls in the message). Then the cipher text was taken out in columns according to a key written across the top of the diagram, but the columns were taken out in alternate fashion, proceeding down the odd columns and up the even ones. Any one of the eight corners of the grille (obverse or reverse) could be placed in the upper left-hand corner.

TOP SECRET ULTRA

The key was derived from a book (in this case the book was never discovered), taking either 13 or 19 letters according to which side of the overlay was uppermost. The page of the book was designated by the first three letters of the indicator, the indicator derived from the normal alphabet:

A B C D E F G H I J
1 2 3 4 5 6 7 8 9 0

A different key was used with every message, and the selection of the page to be used was random, not controlled by the date. The fourth letter was a dummy; the fifth letter indicated the corner of the overlay to be used. Thus,

A B G Z D
1 2 7

would indicate page 127, corner D, and because of the use of D corner, a key length of 13 would be used, since the letters B, D, F, and H signified the possible 13-length keys, and the letters A, C, E, and G the 19-length keys. It was only in the later traffic (See last paragraph) that there appeared the 19-length keys, using the wide face of the grille.

It can be seen that this system although technically only a single transposition, very effectively prevented the usual method of solution by matching the columns. If recognizable nulls were used, solution of a single block or less could perhaps have been effected by fitting these nulls to the known null cells in the diagram. Since there were no stereotyped beginnings and endings on this circuit, the solution of single messages of less than 270 letters presented a difficult problem, so difficult in fact that we never read all of the messages on this circuit.

This traffic was sent over the commercial circuit from Chapultepec, Mexico to Nauen, Germany as well as over the MLENN relay via station VVV TEST (New York) to AOR (Hamburg). The cable addresses BRAJOB and VOLGO were later changed to GESIK and INTER-CIALE. The majority of the traffic was passed over the commercial circuit. The same system was also later discovered in secret ink messages intercepted from couriers out of Mexico. These were labelled by the Germans as "The Max Code."

TOP SECRET ULTRA

2. 3-D BERLIN-RIO DE JANEIRO

In September, 1941, Circuit 3-D stopped using the simple type of transposition and started employing a new type system. As the traffic accumulated, it was examined and the third group of the cipher text was found to be the indicator, being patently the same type of indicator as that encountered in the BRAJOB-BERLIN system. The first three letters of the third group indicated the page of the book to be used; the fourth was a dummy; and the fifth letter gave the corner of the grille:

A B C D E F G H I J
1 2 3 4 5 6 7 8 9 Ø

Thus,

A G I M F
1 7 9

would indicate page 179 for the key, corner F of the grille. If the number of the page was under 100, the two numbers would be indicated either by

H B P W E or Z I E Z A
8 2 9 5

Furthermore, the traffic transmitted on this circuit was divided into blocks of 50 groups (except the first block which had 51 groups because it included the indicator). If the last block was not completely filled, a letter check was given; for example,

1/51 2/50 3/50 4/103

The last group of the cipher text was usually incomplete.

Because the messages were sent in blocks of 50 groups, an overlay with a capacity of 250 letters was first suggested. This seemed somewhat large; half of this figure, or 125 letters, was closer to the length which had been used by the BRAJOB-VOLCO Circuit. The fact that the obvious nulls in messages in the same key coincided fairly well when these messages were lined up in blocks of 125 letters gave confirmation to this theory.

TOP SECRET ULTRA

With a depth of eleven, anagramming was greatly expedited because wrong attempts could quickly be discarded. Trying for the German word ZWO, columns 37, 119, and 67 were brought together giving:

37	119	67
Z	W	O
L	I	S
X	N	X
X	Z	N
F	L	U
I	A	L
O	N	S
C	O	B
X	L	A
V	I	E
E	R	X

This started a second ZWO on line four and suggested VIER on line ten. Anagramming proceeded swiftly and the complete message was recovered. (See Figure 7).

After anagramming, the columns were fitted into a diagram which gave a tentative overlay. Of course the null cells could not be placed exactly until other messages in which a different side or position of the overlay used could be solved. However, with the voluminous amount of traffic transmitted by this particular circuit, solution of the overlay was soon accomplished. (See Figures 8A and 8B). The grille was a diagram of 13 by 19 letters, 125 apertures on each face, all eight corners being used as starting points, with the columns written in alternate vertical transposition, transcribed by a numerical key from a key book. (After the station was closed down in the spy roundup in March, 1942, it was discovered that the book used was a collection of selected stories from the German classics; however, the book was never available to this office.

After the first few messages were decrypted, it was found that there was a serial number given at the beginning of each message, i.e., NR X ZWO X, and it was further discovered that the serial numbering began at the beginning of each month. Thus a very effective crib was brought to light. Not only did the messages have a stereotyped beginning, but the ending usually consisted of either the signature HUMBERTO or ALFREDO. The use of these cribs enabled this office to solve practically all of the messages on this circuit, whether in depth or not.

[illegible]

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85															

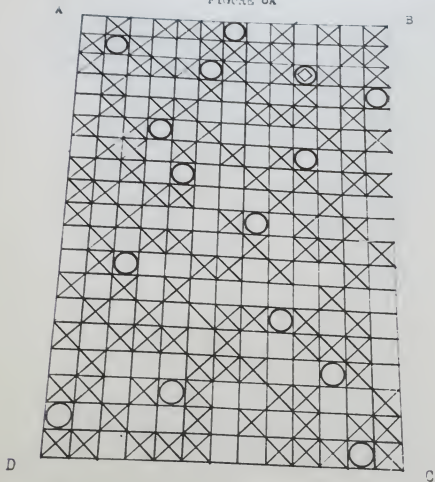
[illegible]


[illegible][illegible]

1
4 0 7 3 6 8
7 0 3 2 8 3 4
1 X T E K O A T
2 X B R I T X P
3 D T X O X " X
4 O N S L A D E
5 A E N X X A A
1 V E R P A C K
2 O M C O N S X
3 D O U G L A S
4 I X B R I T X
5 A D E N D F O
6 A D E N X X A

TOP SECRET ULTRA

FIGURE 8A

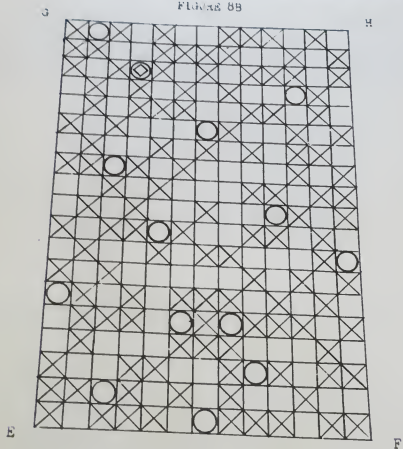


A curious fact developed in the use of this grille by this circuit: namely, the overlay differed in one cell, as used by the control station and outstation. The cell designated by the symbol  was always employed by the control station as a null, but never by the agents in South America.

39

TOP SECRET ULTRA

FIGURE 88



Some of the methods by which messages not in depth were solved are worthy of description. The most common method was by use of the signatures. The best case was that in which, after one or more blocks of 125 letters, there was a remainder of not over 50 letters in length.

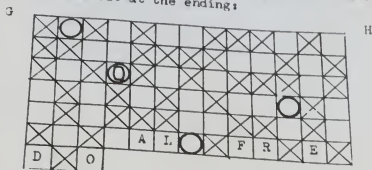
TOP SECRET ULTRA

For example:

Indicator: AATVJ

Remainder: SRRTV BIRXO CSZTA EBUAT XSERA DLXHU EFXUF TXXRO

Inspecting for either of the signatures, it is quickly noted that there is no letter M for HUMBERTO and that all the letters for ALFREDO are present. Blocking off 40 letters (the length of the remainder) on the diagram using the G corner (from the indicator) X ALFREDO is written out at the ending:



In the cipher text it is noted that there are the following number of letters for ALFREDO:

A - 3, F - 2, E - 3, O - 2, L - 1, R - 4, D - 1

Thus the O of ALFREDO can only be placed (arrows indicating direction of the columns)

..... BIRXOCSZTAE TXXRO

And a further examination of the cipher text reveals the placement of the only D and L

..... XSERADL

with one column ending with D and the other starting with L to fit the word ALFREDO. The letters preceding D and the ones following L are filled in; then the final O of the cipher text is inserted. Working backwards on the cipher text, impossible plain text combinations are noted such as H-A-AAIX. The O is therefore a certain;

TOP SECRET ULTRA

		Z				H	J										T
	S		I													X	
R						X										S	
A		X					A					A					A
	C						E										U
D					A	L	B			F	R						E
			O														

The other O (of the possible two in the cipher text) is then tried but this is also discarded because of unlikely German bigrams:

		B		T		H	E					S					
		X		F							U						
	E																
R		X															
A		R				U		S			E					Z	
	A							X								T	
D				X	A	L											

Then the possibility of an X following alphabet in the diagram is attempted:

	L				U							H
	F			X							R	A
	T		X				O				U	
	X										E	
O		A	L	F			R	E		D		

..... RADLX-HU

..... RADLXHUJFXUFTXXRO

a column length of two letters, one ending in F is observed, which would fit for the next two letters following LX4U. Then after EF is placed, XUFT is fitted for one of the columns ending in X. This gives two good bigrams, TH and FE. After XUFT is placed, only four letters remain to make up a column. Because of the assumption of the ending ALFREDO there is only one column in which the four letters can be fitted. Adding XXRO to the diagram, no discrepancies are found.

				X					
T	H				R				
	E	P	X		A				
U			R						
A	I	F	R	O	E	J	C		
X	X								

END IX-11 OF X-11T X-11C

9	10	11	12	13
---	----	----	----	----

[illegible][illegible]

TOP SECRET ULTRA

The foregoing method was also used to solve short messages, the total length of which comprised less than 125 letters. In such cases where the number of the message could be determined from the consecutive numbering system, such as

NR X VIER STEHEN X

solution would be achieved after few trials. The signature HUMBERTO also led to solution more quickly than ALFREDO because of the low frequency letters involved. However, there were exceptions to all these cribs; once in a while the message would end with a number, or a signature other than ALFREDO or HUMBERTO would be used. Key-breaking then became an extremely difficult problem in cases without sufficient depth.

There was another effective way of solving the key besides the use of cribs: placing recognizable nulls in the diagram. For example,

Indicator: AJIZ

Reminder: ZAESK LOEN BZNTG XISES

MXSID NXIFE UENEF EFX

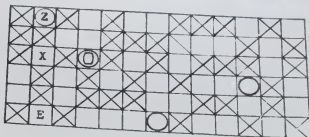
Inspecting for obvious nulls, the following are noted:

ZAESK LOEN BZNTG XISES MXSID NXIFE UENEF EFX

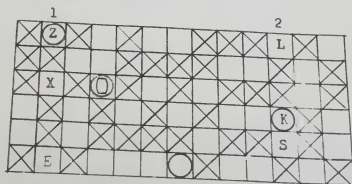
Turning the grille to the "0" corner, the 33 letters of the final section of the cipher text are marked off. It is noted that the first letter of the cipher text is a possible null, which would be a good beginning for column 1. The letter Z from the cipher text is inserted as the null in the top line and the column completed:

TOP SECRET ULTRA

3



Scanning the cipher text again, it is observed that the next possible null should be in column 2 reading upward. There are two columns where this could fit. The column is tried thus:

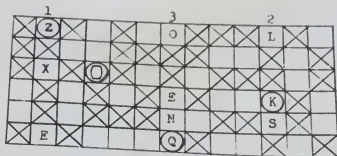


The next possible null is four letters away,

$\begin{array}{c} \text{ZXL} \\ \hline 1 \end{array} \quad \begin{array}{c} \text{SKL} \\ \hline 2 \end{array} \quad \text{OENKZLTP} \dots\dots$

One must necessarily read down a column; there is only one place where this would fit:

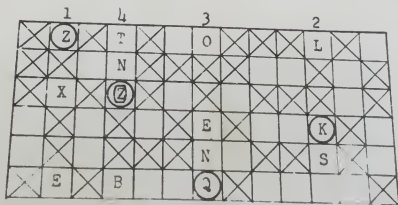
TOP SECRET ULTIMATE



Continuing this process to the next likely null,

ZXE SKL OEN BZNTJ
 1 2 3

there is only one null remaining and the next column can be fitted into only one place:



TOP SECRET ULTRA

There are no discrepancies noted, and inspection of the diagram for possible words, the series S . E 9 strongly suggest the word SIEBEN.

$\frac{242}{1}$ $\frac{SKL}{2}$ $\frac{Och}{3}$ $\frac{JZLF}{4}$ SIEBENS

From the adjacent cipher text the following X is chosen and inserted in the diagram.

	1		4		3		2	5
	Z		T		O		L	3
			N					
X		2						
				E			K	X
				N			S	I
E		B	E	N	Q			

Completing the word SIEBEN the message and key are recovered:

	6	1	10	4	11	12	3	8	9	13	2	7	5
	2			T		F	O				L		G
		E	N						D	E		S	
X		2			E		I					N	
S		F		U		E		N	F		K		X
E		I				N	S			S			I
E		B	E	N	Q			X	X			X	

TOP SECRET ULTRA

This method of placing nulls which appeared obvious proved very successful, both with the end section and with the completely filled grille.

It is interesting also to note the degree of security which the German High Command believed this system possessed. After the rupture in relations between Brazil and Germany and during the period of the Brazilian spy roundup, German Foreign Office dispatches were sent over this circuit in this system, when commercial circuits could no longer be used.

3. 4-D MADRID-WEST AFRICA

In October, 1941 the monitors intercepted a station using the constant call FRK. The traffic had a preamble which was unique:

6/136/141

This was determined to be:

- 6 - date of encipherment
- 136 - total number of letters without indicator
- 141 - total number of letters with indicator

The traffic was examined for an indicator, and this was found to be in the third group (the same place as BRAJOB-VOLCO and Circuit 3-D). Like the circuits previously described, the indicator was derived from the normal alphabet A-J equalling 1-0. The first three or two letters represented the page from which the key was taken, the fourth (sometimes the third) letter a dummy, the fifth evidently a corner of a grille. A frequency count was taken on the cipher text which showed transposition other than German. The longest message was 141 letters (with indicator), and because so many were sent of this length, an overlay with 136 calls (the total number of letters minus the indicator) was suggested. Traffic on this circuit was only intercepted from the control station and was rather scattered, but three messages appeared which had the same key and employed the same corner letter. These messages were lined up in the customary manner (See Figure 9). From the frequency count the messages showed characteristics of being in the Spanish Language; anagramming for this language was then tried. Trying for the Spanish word PARA, columns 44, 66, 45, and 24 were placed together,

TOP SECRET ULTRA

FIGURE 9

		1	2	3	4	5	6	7	8	9	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	3				
1	X	A	X	S	E	X	W	I	P	X	O	P	M	X	U	A	O	C	V	G	C	A	A	C	X	M	J	H	O	
2	S	N	E	B	R	A	X	C	T	N	X	O	A	R	X	X	L	I	C	A	I	A	E	E	I	G	U	O	T	X
3	S	T	L	D	N	O	G	O	E	X	R	O	P	E	X	S	L	A	V	E	M	A	E	E	I	E	G	S	C	E

	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5	5	6		
1	Q	X	X	E	I	E	N	V	N	R	X	R	R	P	R	V	I	O	Z	W	T	I	U	N	R	C	Y	T	I	X
2	R	S	X	M	X	R	A	I	T	U	S	A	V	R	T	R	D	N	X	X	D	E	C	X	T	S	X	E	T	M
3	X	O	A	A	X	T	X	X	S	X	V	A	V	R	T	X	A	A	Z	R	L	I	M	P	O	R	A	L	I	S

	6	6	6	6	6	6	6	6	6	7	7	7	7	7	7	7	7	7	8	8	8	8	8	8	8	8	8	9		
1	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	
2	E	A	M	E	I	A	E	S	T	X	E	K	E	E	X	O	T	D	D	O	R	X	D	X	R	V	E	X	R	M
3	A	E	X	I	G	A	X	I	R	A	X	Y	S	S	X	R	A	X	F	A	E	X	Y	X	X	V	E	X	X	X

	9	9	9	9	9	9	9	9	9	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
1	1	2	3	4	5	6	7	8	9	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1		
2	O	G	R	U	X	X	X	N	E	N	R	A	F	X	X	T	A	I	S	F	S	N	O	O	I	X	N	H	T	
3	X	E	E	X	Y	D	O	E	A	X	X	E	L	A	T	X	I	A	S	X	K	O	A	X	X	T	Y	O	X	D

	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
1	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	
2	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
3	R	O	I	T	S	S	N	O	U	I	F	X	L	P	W	N	-												

1	R	S	V	L	U	S	R	R	O	X	K	A	O	O	T	-
2	X	D	X	E	U	E	R	R	A	X	X	A	A	X	Z	C

TOP SECRET ULTRA

adding an X before and after PAPA,

105	44	66	45	24	106
X	P	A	R	A	X
T	R	A	T	E	X
T	R	A	T	E	X

Continuing this process the messages were completely recovered. (See Figure 10). The overlay could not be completely determined until another message was solved using the other side of the overlay, since this circuit used only four of the possible eight corners, the short side only being used. Using the previously explained method of reconstruction of the grille, the overlay proved to be of the same dimensions as the BRAJOB-VOLGO and Circuit 3-D grilles -- 13 and 19 letters, but it had a capacity of 136 cells. (See Figure 11).

TOP SECRET ULTRA

FIGURE 10

1	0	4	6	4	2	1	0	4	2	2	6	2	2	2	8	1	0	8	1	0	2	6	2	0	8	6	2	2	2	2
2	5	4	6	5	4	6	4	3	3	7	5	5	5	2	8	4	1	7	5	3	4	7	6	8	6	4	4	3	1	9
3	X	P	A	R	A	X	F	R	A	N	C	I	S	C	O	X	X	T	X	A	T	E	T	A	N	X	A	V	I	O
	T	H	A	T	E	X	A	V	E	R	I	G	U	A	R	X	S	I	X	S	E	X	E	N	V	I	A	X	M	A

1	0	4	6	4	2	1	0	4	2	2	6	2	2	2	8	1	0	8	1	0	2	6	2	0	8	6	2	2	2	2
2	2	1	8	7	3	3	2	0	0	7	9	7	1	9	8	2	4	2	1	9	8	0	8	0	9	0	1	1	5	
3	A	R	X	S	I	X	M	O	V	I	M	E	N	T	O	X	B	A	R	C	O	X	S	E	N	X	F	R	E	
	N	E	S	X	D	E	U	S	A	X	U	S	A	X	E	N	X	B	A	R	C	O	X	A	X	T	A	K	O	
	T	E	U	I	A	L	X	D	E	X	G	U	E	R	R	A	X	D	E	X	U	S	A	X	U	S	A	X	E	

1	9	2	1	5	2	1	8	6	7	5	8	9	6	1	1	3	7	1	9	5	3	1	5	7	3	9	3	
2	9	0	8	0	9	6	1	9	1	1	0	7	8	0	2	7	2	6	2	0	9	7	6	2	8	0	7	
3	E	T	O	W	N	X	F	R	E	E	T	O	N	X	H	A	X	D	I	S	M	I	N	U	I	D	O	K
	A	D	I	X	T	A	K	O	R	A	D	I	X	E	N	X	L	A	C	O	S	X	Y	X	S	I	X	
	X	B	A	R	C	O	S	X	A	X	L	A	G	O	S	X	L	A	G	O	S	X	Y	X	S	I	X	

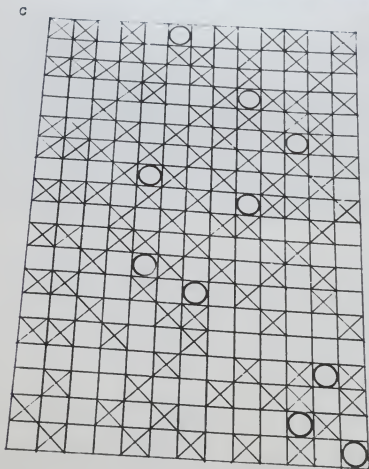
1	1	1	5	3	7	1	9	9	5	3	7	1	3	1	9	5	1	7	4	4	2	2	4	4	5	3	5	6	0
2	8	5	3	3	7	9	3	1	6	8	5	3	4	4	4	5	7	7	4	4	2	2	4	4	5	3	5	6	0
3	N	X	U	L	T	I	N	O	X	T	I	E	M	P	O	X	Y	X	E	N	X	G	U	E	X	P	R	O	
	O	X	C	O	S	T	A	X	D	E	X	O	R	O	X	Y	X	I	X	S	E	X	M	O	N	T	A		
	E	X	M	A	A	E	R	I	A	L	X	S	E	X	T	R	A	I	N	S	P	O	R	T	A	K			

1	9	5	1	1	3	3
2	3	6	6	2	6	3
3	R	C	I	O	N	X
	E	S	T	O	-	X
	E	R	R	O	C	A

44 66 45 24
P A R A
R A T E
R A T E

TOP SECRET ULTRA

FIGURE 11



A

These messages had a fairly consistent crib, beginning usually with PARA X FRANCISCO or CONTINUACION. These cribs gave the beginning of most of the cipher columns, and they could be found in the cipher text and the key determined. Like most of the circuits employing a language other than German, this circuit used X as a separator between each word. It was later determined that if any message contained more than 135 letters, it was split into parts and each part enciphered with a different key.

TOP SECRET ULTRA

E. TRANSPOSITION - SUBSTITUTION

21. MONOALPHABETIC SUBSTITUTION WITH TRANSPOSITION:
HAL-4-N HANBURG-4-N

In February, 1943 attention was first directed to traffic from a station using the fixed call HAL. One message of 73 letters had been intercepted on 1 January, and three more were intercepted in the early part of February. Of these latter three, two were 42 letters—on the same key—and one was 55 letters. The individual frequency tables clearly indicated monoalphabetic substitution with standard alphabet components divided in different positions for each message. Where this substitution was removed from the individual message, the result was found to be transposed plain text. Attempts to anagram simultaneously the two 42-letter messages were rewarded.

In the latter part of February, the F.C.S. provided this office with intercepts from the same station, dated November and December, 1942. Among these were three messages of 55 letters each; and a fifth message of the same length was intercepted at the same time. These five messages of equal length were then superimposed and, having removed the substitution from each of them, the plain text was easily anagrammed in depth, with the first groups of the cipher text remaining unused.

The order in which the letters of the cipher text were written to form the plain text was as follows:

46-8-1-19-28-29-15-33-41-37-16-47-50-32-6-38-13-7-24-23-5-45-9-
2-20-21-44-10-43-11-3-21-26-30-14-34-40-42-12-4-22-25-31-13-35-
39-36-17-48-49

It readily became apparent that this sequence could be written in such fashion as to indicate the transposition diagram and the numeric key employed. It thus developed that the transposition had been effected by means of a Comb diagram, constructed in exactly the same way as by the 3-F Circuit, (D-2,1). In the 4-N Circuit, however, the columnar key proved to be constant. The following diagram shows this numerical sequence written in the comb and the derived numerical and literal keys.

TOP SECRET ULTRA

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	
U	21	46	8	1	19	23	29	15	33	41	37	16	47	50	32	6	38	13	7	24	23																				
E	5	45	9	2	20	27																																			
S	2	19	10																																						
I	9	43		3	21	26	30	14	34	40																															
M	13	42		4	22	25	31	13	35	39	40	17	46	49																											

After this reconstruction of the comb, the longer messages were easily read. The longest message was 68 letters which determined the absolute value of two more letters of the literal key. Combining the fact of the alternating columnar transcription, the seven established letters of the key, and the 21-length numerical keys, the complete literal key was determined to be the proverb, found by consulting the word TREU in the dictionary:

UEB DLEER TREU UND RUDOLPHSEIT

The first group of the cipher text was an indicator for the substitution process. The standard alphabet components were juxtaposed so that the second letter of the indicator was the cipher equivalent of the plain letter in the first position of the indicator—thus producing the substitution alphabet.

The answer station to this control never used radio for reply but was instructed to answer by mail through neutral countries. Judging from the type of information which the control station requested, the agent was located in South America.

E2. POLYALPHABETIC SUBSTITUTION WITH REVERSAL THE SUBSTITUTION

1. 4-1 HXK-URG-BOWENLAK

Traffic of this circuit was first intercepted around the middle of 1942 and proved to be, in the main, simple columnar transposition, employing a width of 16. The solution was the routine general method of fitting sections of the cipher-text together as columns in the original transposition rectangle. However, there were some messages during this period which were in a substitution system. Toward the latter part of 1942, the transposition traffic stopped entirely and it was at first believed that the succeeding traffic was a continuation of the

substitution system previously used. Shortly thereafter, the information on the so-called "Jancowski" (combined transposition and substitution) system was made available to this office; and, after solution of several other "Jancowski" systems, it was discovered that the early substitution traffic had actually been the same as the 16-width transposition with a "Jancowski" substitution superimposed. This fact enabled the complete solution of the traffic up to the point where the transposition traffic ceased entirely.

The traffic which began at this time exhibited no external characteristics of any previously solved system. One fact, which was evident from the beginning of this new type of traffic, was that most of the messages seemed to have very similar beginnings - not continuous repeats, but a high degree of coincidence between all (or almost all) messages at their beginnings. Accordingly, a block of messages were superimposed for their entire length; and it was found that such a superposition gave a degree of coincidence throughout, which could only be consistent with the premise that encipherment in any one position of every message was always by means of the same substitution alphabet.

Dec. 22 152 letters W H G A Y Y J C I D I J X I C I D Y E A V M V Y
 Dec. 24 132 letters W S G R Y J J D I I I I J C G W E J A I V I I
 Dec. 24 159 letters W E S Y J S A J K P I P K A J K E C C C - C

Z H B T H H S C H B D Y J K S D U R K P A V
 F G Z K Y Z P R D C C C K H P F V K S M U
 K W K S F Z Z Z H H S C Z Z Z E I S S P H Z D

K N L M F E W H H H S C L M H P A H H B E T L
 X V I S S R U D N T L A H H H C Y T H R N S U
 G S O J H H B U G A K A V C C C H A P C V

Y C G H X C C C S K K Y T S H O Z H T O H L
 H S S F E L L Z L L H H C C K Z B L R M I
 H G F U U L C C S T E S B F K H X D F H H I

H O M N F S L F O M S V Y H H H B E T L
 K I V C J J F P W C L V P C S H A I J V C S
 B R P E O O F G R D I I S A N S O S M C H A

H H H D Y Z L E H C C C Y Y C L G Y A E
 C H K R C G D U S E Y
 H I S X Z O H Y M S T I H H X Y W V E L

C C C C Y P Y
 H S X I T C C C Y Y

TOP SECRET ULTRA

This superposition of the messages also revealed that there were an extremely large number of cases of two messages having identical letters in alternating positions for varying numbers of positions; so an alternation (so-called "rail-fencing") treatment was clearly indicated. When all the messages were so treated (i.e. writing the odd-position letters in succession on one line, and the even-position letters in succession on the line below), long repeats developed at the beginnings of the messages and additional repeats were found throughout the messages - both in identical positions and in different positions. At first, it appeared that the recurrence of any repeat was independent of its position in the message; but, on closer study, it became evident that each recurrence depended on whether the position was odd or even (with reference to the "rail-fenced" version of the messages). That is to say, the intervals between the positions of any occurrences of a repeat were always a multiple of 2.

At this point, it seemed evident that there was just a two-alphabet substitution involved in alternating positions (with reference to the "rail-fenced" version of the messages). But when combined frequency counts were made on the letters in each of the two classes of positions, the coincidence was higher than random but not high enough for monoalphabeticity. Nor did a digraphic frequency count exhibit a degree of coincidence high enough for monoalphabeticity, although this also was much higher than random.

Further study of the positions of repeats finally disclosed the fact that there were ranges within each message within which certain repeats never occurred; and, in general, that there seemed to be two groups of repeats - each of which recurred within distinct and mutually exclusive ranges within each message. Continued study, together with a modicum of trial and error, then reduced these ranges to alternating 12-letter double-line blocks of the "rail-fenced" version of the messages.

TOP SECRET ULTRA

"PLAIN-TEXT" VERSION:

152	WQYJIIKCDPVV	EHSEBYKEUKH
	WAFCDJIIYANR	HTHNRJSDRPV
132	WYJIIKCDMII	TYFPHDCFTFKN
	WJBBVJRSVW	GKEDRBNMVHV
10	WYYSJEBKJSS-	KKEDHSZBIMPZ
	WJAXIFAKCCE	WSEHSZBNSHD
	YLFWMELMNNNSF	YGRXBKYSOHGL
	KMBMNGNFHRTL	CHGZSATHZTHU
	XESUNLNNKNNB	HSZIFXUKKLHB
	VBDTXNGTRNB	BFZPLHZCGRHD
	GOMBGAVWSAOS	HPUNKTTFHNBKK
	SJMUFWNCFXK	GULOSBBKXFHU
	NMFLOSVMNPJP	HUYLNBKKXKEM
	NSFWUNNSIGQ	HDZHDRIYWGKMV
	FVJFPOQVSSRJS	CKFDNK
	ISJWWEFWHLVS	DRGUSY
	EPOSKOPBNONH	HSZBYSLHYFZQ
	RZOGXIWASSGA	LXDRHUHZADNF
	HGYD	
	CCPY	
	HXTBWAQ	
	SIESOVY	

It was then discovered that, by considering each set of these blocks separately, the combined frequency counts of alternating letters were unquestionably monoalphabetic. It then became an easy task to recover each of the four monoalphabets so segregated. It was then discovered that the alphabets were key-word-mixed alphabets, with some minor variation introduced into their derivation by some eccentric means of locating certain letters. Also, the pair of alphabets used for each set of 12-letters double-line blocks were both derived from the same key word, but with the juxtaposition of plain and cipher components varied for each alphabet. (See Figure 12.)

Although the procedure used in enciphering this traffic was cryptographically complicated, but was rather complex mechanically, the following recapitulation of the enciphering procedure

should provide clarification of the mechanics of the system. The plain text was written out in lines of 12 letters each, one under the other. Substitution was then performed with Alphabet 1 on the 1st, 3rd, 5th, 7th, 9th and 11th letters of the 1st, 3rd, 5th, etc. pairs of lines; with Alphabet 2 on the 2nd, 4th, 6th, 8th, and 10th letters of the same pairs of lines; with Alphabet 3 on the 1st, 3rd, 5th, 7th, 9th, and 11th letters of the 2nd, 4th, 6th, etc. pairs of lines; and with Alphabet 4 on the 2nd, 4th, 6th, 8th, 10th, and 12th letters of the same pairs of lines. Following the substitution, the cipher-text was transcribed TAKING the successive vertical pairs of the 1st pair of lines, then of the 2nd pair of lines, and so on (i.e., "rail-fencing" each pair of lines of the cipher-text).

It was not until the details of "Verfahren 40" were known that an approximation of the method of substitution was derived. The following may not be the true method used in this system, but it is the only one so far conceived which will explain the alterations in an otherwise normal key word-mixed alphabet. Suppose the key word-mixed alphabets used for the March, 1943 traffic to be written in 5 x 5 squares with the letter "J" arbitrarily placed outside the squares as indicated:

<u>Alphabet 1</u>	<u>Alphabet 2</u>	<u>Alphabet 3</u>	<u>Alphabet 4</u>
D E U T S J	D E U T S	S O W E T	S O W E T
C H L A N	C H L A N	R U Z L A J	R U Z L A
F G I K	F G I K	N D F C F	N D F C F
P O P R	P O P R	G H I K M	G H I K M
V W X Y Z	V W X Y Z	P Q V X Y	P Q V X Y
	J		J

Thus, for Alphabets 1 and 3, the equivalent of each plain text letter is found by counting 3 letters to the right (continuing from the end of one line to the beginning of the next, and from the end of the last line to the beginning of the first). Similarly, for alphabets 2 and 4, the equivalent of each plain text letter is found by counting 3 letters downward (continuing from the bottom of one column to the top of the one to the left, and from the bottom of the extreme left to the top of the extreme right). This seems to be the greatest degree of simplification possible with these alphabets, as well as the only way possible of ciphering by means of an un-distorted key word-mixed sequence.

FIGURE 12

DECRYPTED VERSION

1st (Cipher)
(Plain)

1 2 3 4 5 6 7 8 9 10 11 12 13

1 2 3 4 5 6 7 8 9 10 11 12 13

W O Y J I I K C D V V

I B E S E D Y K N U N

H R I Z W O Z W O N V L

H B R I N S K E T E S A

H A K C D J I I Y A N R

H T H H H D J S O S F V

L X Z W O Z W O I X T R D

H G E V R R K I N H Q L

K L P W H E L M N H S F

Y O X X B K Y S O R O L

L A C H L A O B E T R I

H Z W O T E I I M A V F

H M R H H G E P E R T L

C N O Z S K T H Z T H Z

H B S B E R E I T D A S

B A U X O E F A N O R H

H M P L O S V N H B J P

H U Y L N B K K I K R H

H B C S H E U T E N I C

H N X F A S S E R W E I T

O H S P W U N H S I O Q

H D Z H D R I W O K M V

H T R I N G E T R O P F

H R N A C H X M U E L L

H O Y D

H E R I K

H C C P Y

H B W M X

132

W O Y J I I K C D J I I

F Z Y P H D C K P P K N

H R I Z W O Z W O Z W O

H R I X C E R B E R U S W

S R J B B K J R S A V W

O K Z E D R B H M V H U

H R D I N S V I D R X U H

H U E N S C H T A L L E N

X I S U N L N K N K N B

H S Z L F I U K K L H B

V O R G E S E T Z T E N

H E I N F R O H E S P E S

V B E D T X N G T R N B

B P Z Q L H Z C B R H D

H U N D K A M E R A D E N

H T U N D D A N K T H E R

K V J P O Q V S S R J S

C K Y D N K

Z L I C H F U E R D I E

H B E R R A E

I S J W N E W W H L V S

H D R O U S Y

H E I N N A C H T S U E

H C H U N O P

FIGURE 12 CONTINUED

7
150

W Q Y S J B B K J S S -	K K V E H S S B I M P E
H P X E I N S V I E R -	S E R X E I N S S V O Z
D S J A X I P A K C C E	W S E B E E E E W S E D
O E I X V O W X E W B A	V I N S E I N S V I E R
G O N B O A V W S A O S	H P U M K I F F F B K K
F U E N P I U H R Z H E	A C H T S O R U S S E
S J M U F W H C N F I B	G U L O S B B K X P H U
E Z L O C H E W E I V H	U N D B O S T E W U R H
B P O S K O P B W O N H	H S Z B Y S L H Y F Z Q
S C H E Z U M N K U E J	E I N S I D A X U N D
R E O G I W A S S G A	L X O R H U H Z B D N Y
J A H R V O N X R E F X	D O M A N N E X T R A U
H X T B W A Q	
T M A N N I P	
S I E S O V Y	
R O D E H L X	

DECIPHERING ALPHABETS:

(Cipher) A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

(Plain)

1	K S B O D C F T W I T G L E H M P J R A Q U N V X Y
2	X N W K A I R J O Z V S B T U C F D E Y G L H M P Q
3	Y T B C I R U E Z K S D L A M O P J G F H Q V W X N
4	V S E R J U Z A Y Q E F T W B C D H I J N L M O P X

WRITTEN AS KEYWORD MIXED:

(Plain) (J) K A T H O D E N W I (J) R S B C F G L M P Q U V X Y Z

(Cipher:)

1	A T H O D E N W I (J) R S B C F G L M P Q U V X Y Z K
2	H D E N W I R S B C F G L M P Q U V X Y Z O K A T (J)

(Plain) (J) A N Z I E H U G S K (J) R F T B C D L M O P Q V W X Y

(Cipher:)

3	N Z I E H U G S K (J) R F T B C D L M O P Q V W X Y A
4	E H U G S K R F T R C D L M O P Q V W X Y (J) A N Z I

TOP SECRET

E3. POLYALPHABETIC SUBSTITUTION WITH COLUMNAR
TRANSPOSITION: JANOWSKI METHOD

In December, 1942, a record of the case of a German agent apprehended the previous month by the Royal Canadian Mounted Police was made available to this office. The record contained a good back round on the German Intelligence Service together with an account of the cipher system to be employed by the agent. He had two novels with him; one was to be selected and used for call signs and keys for the system, the selection to be made after contact was achieved. The agent's number (in this particular case 28) added to the date of the month and number of the month gave the page of the book to be used. Two different preamble keys were also included — one for the first four groups to contain the transmission date, time, letter check, and serial number of the message, the second key for the fifth group alone to contain the enciphering date. The calls were extracted from the page of the day reading from the lower left hand corner upwards for the control, from the lower right hand corner upwards for the answer station. The text was first written horizontally into a transposition diagram, using a 20 length key derived from the first 20 letters reading downwards from the top left-hand corner of the page for the day indicated. Then the columns were taken out vertically according to the transposition key, each column substituted by means of a substitution key which was derived from the first twenty letters, reading downwards, of the page for the first of each month, the substitution key remaining constant for a month. The reference letter used to effect the substitution was the letter in the top left hand corner of the page for the day indicated. Thus, on the first day of the month, both the substitution and transposition keys were the same. For example, taking a different substitution and transposition key:

Transposition key - W R V C S L P T H F A S F P A A G A A Q
(1st 20 letters
reading down)

W R V C S L P T H F A S F P A A G A A Q
20 15 19 5 16 10 12 18 9 6 1 17 7 13 2 3 8 11 4 14

Text—

20 15 19 5 16 10 12 18 9 6 1 17 7 13 2 3 8 11 4 14
F E L R E W I L N E L M K H A Y R Y X X
I O H B I N S E H R G M T X X W I E G E
N T S M I T I H N L M K A S E R Z L I C
L E T E U E S S E L S L T E T O L T A A

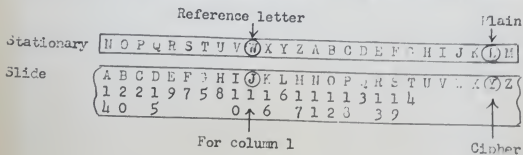
TOP SECRET

T W B T H K G K M A T H T M J T B J T B
14 20 2 15 9 7 5 8 10 1 16 6 17 11 12 18 3 13 19 4

The substitution key is then written under the first twenty letters of the standard alphabet:

A B C D E F G H I J K L M N O P Q R S T etc.
14 20 2 15 9 7 5 8 10 1 16 6 17 11 12 18 3 13 19 4

This is slid against a stationary standard alphabet, using the reference letter (the first letter on the top left hand corner of the page for the day) for a setting, reading the cipher letter to be obtained on the slide under the plain text letter in the stationary alphabet. In this case W is the reference letter. To substitute column 1 of the diagram, the letter numbered 1 on the substitution slide is set under W on the stationary alphabet:



Column 1 - $\frac{1}{L}$
G
N
O

Substituted - $\frac{1}{Y}$
T
A
D

Column 2 from the diagram would be substituted with letter C placed under reference W, column 3 with letter Q placed under W, etc.

Two frequencies each were designated for the control and answer stations, different calls to be used on each frequency. A few messages had been intercepted on this case, but coverage was immediately discontinued because the station was being covered by the Royal Canadian Mounted Police. It was also interesting to note that the agent was told to insert the letter U in triplicate in the signal group in the event that he became controlled; however,

TOP SECRET ULTRA

he had confessed this detail before any messages were sent by the Canadians. The first messages intercepted were studied to determine the actual application of the system.

1. 4-M HAMBURG-SPAIN

In January, 1943, a station similar to the Hamburg station came on the air and sent two messages with the usual clandestine procedure. Two days after the first transmission, the station came on the air again using different calls and sent two messages. When the messages were compared, it was found that the messages of both transmissions were of the same length and that the second transmissions was obviously a repetition of the first but with a different encipherment. Further examination revealed a startling discovery: both messages of the first transmission tested for substitution, while the first message of the second transmission tested for transposition, the second message for substitution. When the two versions of the message were superimposed and a segment of the transposition text was found repeated in the substituted version, it was immediately found that each segment of the transposition version could be extended on the normal alphabet component to produce a segment of the substitution version. This automatically stripped off the substitution, determined the number of columns, and fixed the long and short columns--all in one operation--as well as verifying the Janowski type of substitution. The only remaining step necessary was that of anagramming one message. Thereby the two keys were recovered simultaneously. Both messages were in Spanish and concerned the establishment of an agent station and methods of reporting.

This particular case was one of the most flagrant violations of cryptographic security encountered, and deserves particular comment because it was committed by the controlling station. Unfortunately, no further traffic was intercepted on this circuit after the initial messages. However, the two messages served to give notice that the system provided for the agent in Canada would probably be widely used by Hamburg.

2. 4-L HAMBURG-GIJON

After the situation encountered in Circuit 4-M, traffic which had been intercepted for a short time on another new circuit was inspected for the possibility of being in the new type Hamburg system. The cipher text contained groupings of letters which indicated that a different substitution had been made on

each column, i.e.,

V B R S N C C C C L L L O Y V etc.

The first four groups were found to contain the customary preamble, and the fifth group was believed to have the enciphering date in the last two letters. The cipher text for the second message intercepted on this circuit (132 letters without the first five groups) was run off on an I.B.M. tabulation with the plain component completed for each letter (See Figure 13). Acting on the theory that a twenty-length key was employed, the text was marked off into tentative columns, allowing for eight columns of six letters each and twelve columns of seven letters each. Because the language was unknown, generatrices were then selected on the basis of both German and Spanish. The best possible generatrix for each column was marked in red for German, in green for Spanish. (See Figure 13). The generatrices were marked for six or seven letters which were best for plain text, but if this fell a little above or below the tentative divisions it made no difference. Sometimes the generatrix selected would be equally as good for Spanish as it would for German, as in the case of columns 19 and 20 (See Figure 13). After the best generatrices were selected, anagramming was then attempted. Taking the red columns 4 and 5 (See Figure 13) because of letters C and H:

4	5
S	P
A	G
E	I
C	H
C	H
L	S

it was found that all combinations fitted well. The, adding red column 11, (Figure 13),

11	4	5
S	S	P
R	A	G
W	E	I
C	C	H
I	C	H
U	L	S

TOP SECRET ULTRA

FIGURE 13.

PLAIN COMPONENT COMPLETED

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
1	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
2	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
3	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
4	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
5	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
6	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

TOP SECRET ULTRA

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
2	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
3	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
4	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
5	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
6	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
7	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
8	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
9	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
10	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
13	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K

FIGURE 13- CONTINUED

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
14	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
15	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
16	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
17	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
18	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
19	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

TOP SECRET ULTRA

FIGURE 3- CONTINUED

20

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

TOP SECRET ULTRA

FIGURE 11

COLUMNS AND GENERATRICES CORRECTED

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
1	J	V	A	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	J	V	A	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
3	J	V	A	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4	J	V	A	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
5	J	V	A	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
6	J	V	A	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

73

[illegible]

TOP SECRET ULTRA

FIGURE 14 - CONTINUED

[illegible]

TOP SECRET ULTRA

FIGURE 14 - CONTINUED

20

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

TOP SECRET ULTRA

Numerical weights were assigned to each letter of the alphabet on the basis of their frequency according to language. In this case German was the language on which the frequencies were made. The weights were assigned thus:

A	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
B	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
C	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0

I. cards were then punched for each letter of the alphabet, i.e., for letter A, with the letter itself at the top, the complete series of numerical equivalents starting with 63 (for A) through 50 (for Z); for the letter B, starting with 54 (for B) through 63 (for A), etc.

The total length of the message was divided by twenty (the length of the key) in the usual way to get the column lengths. The long and short columns were placed fairly evenly throughout the message. This, of course, caused a margin of error by placing some letters in columns where they did not belong, but not enough error was introduced to affect seriously the final calculation. Then cards were taken from those previously prepared, one for each cipher text letter, with a separator card at the end of each assumed column. For example, in the message shown in Figure 15, the cipher text is the first column, and we would select cards P, B, J, B, Y, G, P, U, L, G, and then a separator card, etc. When these cards were totalled on the tabulator, adding the 25 2-column fields simultaneously, they were added by columns, producing the sums shown in Figure 16 (with two figures only of the sum being shown):

	1	2	3	4	24	25	26
(1)	47	22	66	63	etc.									
(2)	54	57	58	74										
(3)	25	47	60	55										
(4)	54	57	58	74										
(5)	24	50	63	54										
(6)	58	60	55	25										
(7)	47	72	66	63										
(8)	62	45	51	63										
(9)	60	55	69	57										
(10)	30	60	65	25										
	148	477	627	557										

TOP SECRET ULTRA

FIGURE 15

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	J	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Y	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	P	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
2	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
3	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
5	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G

FIGURE 15 - CONTINUED

TOP SECRET ULTRA

127456789D1115151617181920212223242526
 N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
 D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
 Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
 L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
 Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
 U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
 H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
 E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
 I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
 Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
 L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
 K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
 C D E F G H I J K L M N O P Q R S T U V W X Y Z A
 U V W X Y Z A B C D E F G H I J K L M N O P Q R S
 D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
 Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
 I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
 U V W X Y Z A B C D E F G H I J K L M N O P Q R S
 L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
 S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
 F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
 I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
 P C D E F G H I J K L M N O P Q R S T U V W X Y Z A
 R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
 I M N O P Q R S T U V W X Y Z A B C D E F G H I J K
 S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
 W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
 W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
 V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
 H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
 T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
 G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
 T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
 T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
 T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

5
 6
 7
 8
 9

10
 11
 12
 13
 14
 15
 16
 17
 18
 19
 20
 21
 22
 23
 24
 25
 26
 27
 28
 29
 30
 31
 32
 33
 34
 35
 36
 37
 38
 39
 40
 41
 42
 43
 44
 45
 46
 47
 48
 49
 50
 51
 52
 53
 54
 55
 56
 57
 58
 59
 60
 61
 62
 63
 64
 65
 66
 67
 68
 69
 70
 71
 72
 73
 74
 75
 76
 77
 78
 79
 80
 81
 82
 83
 84
 85
 86
 87
 88
 89
 90
 91
 92
 93
 94
 95
 96
 97
 98
 99
 100
 101
 102
 103
 104
 105
 106
 107
 108
 109
 110
 111
 112
 113
 114
 115
 116
 117
 118
 119
 120
 121
 122
 123
 124
 125
 126
 127
 128
 129
 130
 131
 132
 133
 134
 135
 136
 137
 138
 139
 140
 141
 142
 143
 144
 145
 146
 147
 148
 149
 150
 151
 152
 153
 154
 155
 156
 157
 158
 159
 160
 161
 162
 163
 164
 165
 166
 167
 168
 169
 170
 171
 172
 173
 174
 175
 176
 177
 178
 179
 180
 181
 182
 183
 184
 185
 186
 187
 188
 189
 190
 191
 192
 193
 194
 195
 196
 197
 198
 199
 200
 201
 202
 203
 204
 205
 206
 207
 208
 209
 210
 211
 212
 213
 214
 215
 216
 217
 218
 219
 220
 221
 222
 223
 224
 225
 226
 227
 228
 229
 230
 231
 232
 233
 234
 235
 236
 237
 238
 239
 240
 241
 242
 243
 244
 245
 246
 247
 248
 249
 250
 251
 252
 253
 254
 255
 256
 257
 258
 259
 260
 261
 262
 263
 264
 265
 266
 267
 268
 269
 270
 271
 272
 273
 274
 275
 276
 277
 278
 279
 280
 281
 282
 283
 284
 285
 286
 287
 288
 289
 290
 291
 292
 293
 294
 295
 296
 297
 298
 299
 300
 301
 302
 303
 304
 305
 306
 307
 308
 309
 310
 311
 312
 313
 314
 315
 316
 317
 318
 319
 320
 321
 322
 323
 324
 325
 326
 327
 328
 329
 330
 331
 332
 333
 334
 335
 336
 337
 338
 339
 340
 341
 342
 343
 344
 345
 346
 347
 348
 349
 350
 351
 352
 353
 354
 355
 356
 357
 358
 359
 360
 361
 362
 363
 364
 365
 366
 367
 368
 369
 370
 371
 372
 373
 374
 375
 376
 377
 378
 379
 380
 381
 382
 383
 384
 385
 386
 387
 388
 389
 390
 391
 392
 393
 394
 395
 396
 397
 398
 399
 400
 401
 402
 403
 404
 405
 406
 407
 408
 409
 410
 411
 412
 413
 414
 415
 416
 417
 418
 419
 420
 421
 422
 423
 424
 425
 426
 427
 428
 429
 430
 431
 432
 433
 434
 435
 436
 437
 438
 439
 440
 441
 442
 443
 444
 445
 446
 447
 448
 449
 450
 451
 452
 453
 454
 455
 456
 457
 458
 459
 460
 461
 462
 463
 464
 465
 466
 467
 468
 469
 470
 471
 472
 473
 474
 475
 476
 477
 478
 479
 480
 481
 482
 483
 484
 485
 486
 487
 488
 489
 490
 491
 492
 493
 494
 495
 496
 497
 498
 499
 500
 501
 502
 503
 504
 505
 506
 507
 508
 509
 510
 511
 512
 513
 514
 515
 516
 517
 518
 519
 520
 521
 522
 523
 524
 525
 526
 527
 528
 529
 530
 531
 532
 533
 534
 535
 536
 537
 538
 539
 540
 541
 542
 543
 544
 545
 546
 547
 548
 549
 550
 551
 552
 553
 554
 555
 556
 557
 558
 559
 560
 561
 562
 563
 564
 565
 566
 567
 568
 569
 570
 571
 572
 573
 574
 575
 576
 577
 578
 579
 580
 581
 582
 583
 584
 585
 586
 587
 588
 589
 590
 591
 592
 593
 594
 595
 596
 597
 598
 599
 600
 601
 602
 603
 604
 605
 606
 607
 608
 609
 610
 611
 612
 613
 614
 615
 616
 617
 618
 619
 620
 621
 622
 623
 624
 625
 626
 627
 628
 629
 630
 631
 632
 633
 634
 635
 636
 637
 638
 639
 640
 641
 642
 643
 644
 645
 646
 647
 648
 649
 650
 651
 652
 653
 654
 655
 656
 657
 658
 659
 660
 661
 662
 663
 664
 665
 666
 667
 668
 669
 670
 671
 672
 673
 674
 675
 676
 677
 678
 679
 680
 681
 682
 683
 684
 685
 686
 687
 688
 689
 690
 691
 692
 693
 694
 695
 696
 697
 698
 699
 700
 701
 702
 703
 704
 705
 706
 707
 708
 709
 710
 711
 712
 713
 714
 715
 716
 717
 718
 719
 720
 721
 722
 723
 724
 725
 726
 727
 728
 729
 730
 731
 732
 733
 734
 735
 736
 737
 738
 739
 740
 741
 742
 743
 744
 745
 746
 747
 748
 749
 750
 751
 752
 753
 754
 755
 756
 757
 758
 759
 760
 761
 762
 763
 764
 765
 766
 767
 768
 769
 770
 771
 772
 773
 774
 775
 776
 777
 778
 779
 780
 781
 782
 783
 784
 785
 786
 787
 788
 789
 790
 791
 792
 793
 794
 795
 796
 797
 798
 799
 800
 801
 802
 803
 804
 805
 806
 807
 808
 809
 810
 811
 812
 813
 814
 815
 816
 817
 818
 819
 820
 821
 822
 823
 824
 825
 826
 827
 828
 829
 830
 831
 832
 833
 834
 835
 836
 837
 838
 839
 840
 841
 842
 843
 844
 845
 846
 847
 848
 849
 850
 851
 852
 853
 854
 855
 856
 857
 858
 859
 860
 861
 862
 863
 864
 865
 866
 867
 868
 869
 870
 871
 872
 873
 874
 875
 876
 877
 878
 879
 880
 881
 882
 883
 884
 885
 886
 887
 888
 889
 890
 891
 892
 893
 894
 895
 896
 897
 898
 899
 900
 901
 902
 903
 904
 905
 906
 907
 908
 909
 910
 911
 912
 913
 914
 915
 916
 917
 918
 919
 920
 921
 922
 923
 924
 925
 926
 927
 928
 929
 930
 931
 932
 933
 934
 935
 936
 937
 938
 939
 940
 941
 942
 943
 944
 945
 946
 947
 948
 949
 950
 951
 952
 953
 954
 955
 956
 957
 958
 959
 960
 961
 962
 963
 964
 965
 966
 967
 968
 969
 970
 971
 972
 973
 974
 975
 976
 977
 978
 979
 980
 981
 982
 983
 984
 985
 986
 987
 988
 989
 990
 991
 992
 993
 994
 995
 996
 997
 998
 999
 1000
 1001
 1002
 1003
 1004
 1005
 1006
 1007
 1008
 1009
 1010
 1011
 1012
 1013
 1014
 1015
 1016
 1017
 1018
 1019
 1020
 1021
 1022
 1023
 1024
 1025
 1026
 1027
 1028
 1029
 1030
 1031
 1032
 1033
 1034
 1035
 1036
 1037
 1038
 1039
 1040
 1041
 1042
 1043
 1044
 1045
 1046
 1047
 1048
 1049
 1050
 1051
 1052
 1053
 1054
 1055
 1056
 1057
 1058
 1059
 1060
 1061
 1062
 1063
 1064
 1065
 1066
 1067
 1068
 1069
 1070
 1071
 1072
 1073
 1074
 1075
 1076
 1077
 1078
 1079
 1080
 1081
 1082
 1083
 1084
 1085
 1086
 1087
 1088
 1089
 1090
 1091
 1092
 1093
 1094
 1095
 1096
 1097
 1098
 1099
 1100
 1101
 1102
 1103
 1104
 1105
 1106
 1107
 1108
 1109
 1110
 1111
 1112
 1113
 1114
 1115
 1116
 1117
 1118
 1119
 1120
 1121
 1122
 1123
 1124
 1125
 1126
 1127
 1128
 1129
 1130
 1131
 1132
 1133
 1134
 1135
 1136
 1137
 1138
 1139
 1140
 1141
 1142
 1143
 1144
 1145
 1146
 1147
 1148
 1149
 1150
 1151
 1152
 1153
 1154
 1155
 1156
 1157
 1158
 1159
 1160
 1161
 1162
 1163
 1164
 1165
 1166
 1167
 1168
 1169
 1170
 1171
 1172
 1173
 1174
 1175
 1176
 1177
 1178
 1179
 1180
 1181
 1182
 1183
 1184
 1185
 1186
 1187
 1188
 1189
 1190
 1191
 1192
 1193
 1194
 1195
 1196
 1197
 1198
 1199
 1200
 1201
 1202
 1203
 1204
 1205
 1206
 1207
 1208
 1209
 1210
 1211
 1212
 1213
 1214
 1215
 1216
 1217
 1218
 1219
 1220
 1221
 1222
 1223
 1224
 1225
 1226
 1227
 1228
 1229
 1230
 1231
 1232
 1233
 1234
 1235
 1236
 1237
 1238
 1239
 1240
 1241
 1242
 1243
 1244
 1245
 1246
 1247
 1248
 1249
 1250
 1251
 1252
 1253
 1254
 1255
 1256
 1257
 1258
 1259
 1260
 1261
 1262
 1263
 1264
 1265
 1266
 1267
 1268
 1269
 1270
 1271
 1272
 1273
 1274
 1275
 1276
 1277
 1278
 1279
 1280
 1281
 1282
 1283
 1284
 1285
 1286
 1287
 1288
 1289
 1290
 1291
 1292
 1293
 1294
 1295
 1296
 1297
 1298
 1299
 1300
 1301
 1302
 1303
 1304
 1305
 1306
 1307
 1308
 1309
 1310
 1311
 1312
 1313
 1314
 1315
 1316
 1317
 1318
 1319
 1320
 1321
 1322
 1323
 1324
 1325
 1326
 1327
 1328
 1329
 1330
 1331
 1332
 1333
 1334
 1335
 1336
 1337
 1338
 1339
 1340
 1341
 1342
 1343
 1344
 1345
 1346
 1347
 1348
 1349
 1350
 1351
 1352
 1353
 1354
 1355
 1356
 1357
 135

FIGURE 15 - CONTINUED

FIGURE 15 - CONTINUED

10

11

12

13

113

TOP SECRET ULTRA

TABLE 15 - CONTINUED

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
14	P	Y	B	K	L	M	N	O	X	C	D	G	J	K	L	M	N	O	X	C	D	G	J	K	L	M	N
	Y	B	K	L	M	N	O	X	C	D	G	J	K	L	M	N	O	X	C	D	G	J	K	L	M	N	
	B	K	L	M	N	O	X	C	D	G	J	K	L	M	N	O	X	C	D	G	J	K	L	M	N		
	K	L	M	N	O	X	C	D	G	J	K	L	M	N	O	X	C	D	G	J	K	L	M	N			
	L	M	N	O	X	C	D	G	J	K	L	M	N	O	X	C	D	G	J	K	L	M	N				
	M	N	O	X	C	D	G	J	K	L	M	N	O	X	C	D	G	J	K	L	M	N					
	N	O	X	C	D	G	J	K	L	M	N	O	X	C	D	G	J	K	L	M	N						
	O	X	C	D	G	J	K	L	M	N	O	X	C	D	G	J	K	L	M	N							
	X	C	D	G	J	K	L	M	N	O	X	C	D	G	J	K	L	M	N								
	C	D	G	J	K	L	M	N	O	X	C	D	G	J	K	L	M	N									
	D	G	J	K	L	M	N	O	X	C	D	G	J	K	L	M	N										
	G	J	K	L	M	N	O	X	C	D	G	J	K	L	M	N											
	J	K	L	M	N	O	X	C	D	G	J	K	L	M	N												
	K	L	M	N	O	X	C	D	G	J	K	L	M	N													
	L	M	N	O	X	C	D	G	J	K	L	M	N														
	M	N	O	X	C	D	G	J	K	L	M	N															
	N	O	X	C	D	G	J	K	L	M	N																
	O	X	C	D	G	J	K	L	M	N																	
	X	C	D	G	J	K	L	M	N																		
	C	D	G	J	K	L	M	N																			
	D	G	J	K	L	M	N																				
	G	J	K	L	M	N																					
	J	K	L	M	N																						
	K	L	M	N																							
	L	M	N																								
	M	N																									
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										
	X																										
	C																										
	D																										
	G																										
	J																										
	K																										
	L																										
	M																										
	N																										
	O																										

WFOH 15 - INT. 1000

10

TOP SECRET ULTRA

The correct generatrix was usually one of the two or three highest sums, although not necessarily the highest. In Figure 16, the highest sums for each assumed cipher column are ringed in black, the second highest (if necessary) is ringed in green, and the correct one in red. Out of twenty columns, ten of the highest sums were actually the correct generatrices, three of the highest best were also correct. The same principles mentioned before helped out here, namely, that one a generatrix is chosen as the correct one for a column, it cannot be chosen again for any other column, and that the six generatrices not chosen must appear in a complete block.

Just before this circuit changed over to a newer type system, a copy of the book employed for the keys was obtained by this office, thus reducing solution to a purely cryptographic problem. The book used was "L'ANCIEN DU MISERICORDIE" in French. This circuit was the only one for which the key book was available to this office during its use.

4. 4-F HAMBURG-LIBON

In March, 1943, on almost the same day as circuit 4-F stopped using the five-group preamble, circuit 4-F, which up to this time employed the running-key substitution system with the first five groups containing the preamble, changed over to this type system. As in the case of circuit 4-F, circuit 4-F also used an indicator in the fifth group, the last two letters of this group indicating the enciphering date, the first two letters, the line for the page of the day in the key book. This circuit also used a twenty-length key for both the transposition and the substitution, and solution was readily achieved by completing the plain component and using the runs based on German weights.

5. 4-R HAMBURG-VIGO

Circuit 4-R was first intercepted in April, 1943, as the first examination of traffic revealed groupings of letters which indicated an encipherment by columns using the "Janowski" method. Like circuits 4-F and 4-F, circuit 4-R employed the fifth group of the cipher text for an indicator, giving the date of encipherment. The same methods of attack which were employed on the previously described circuits were used in this instance as well, both keys being twenty letters in length.

TOP SECRET ULTRA

FIGURE 16

FIGURE 16

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z			
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26			
1-	48	47	62	55	52	54	61	56	53	51	56	54	56	56	56	55	59	48	61	49	54	55	50	58	50	59	43		
2-	51	52	48	46	44	46	50	55	51	57	42	52	53	53	43	40	43	46	53	57	49	40	45	59	43	59	43		
3-	44	46	51	49	50	43	48	51	55	52	51	39	43	52	45	55	51	47	45	50	39	47	55	49	53	50	51		
4-	54	56	49	50	57	58	55	48	53	57	52	49	58	59	45	57	53	51	50	57	59	49	51	56	53	54	51		
5-	50	52	49	45	45	45	49	53	47	50	49	48	51	46	56	56	45	45	50	49	44	47	53	45	49	51	54	48	47
6-	48	47	48	53	49	39	49	52	44	51	55	45	44	50	49	50	49	44	47	53	45	49	51	54	48	47	51		
7-	51	49	51	50	45	48	47	50	46	54	50	49	52	37	48	46	47	48	52	55	50	40	49	51	45	48	51		
8-	57	56	53	53	50	54	52	52	56	58	55	54	55	48	50	55	54	52	54	53	46	57	62	54	46	55	51		
9-	55	51	44	43	46	40	51	55	50	42	47	52	55	53	43	35	47	45	52	56	47	40	45	55	53	51			
10-	51	54	50	51	50	45	54	44	44	47	49	47	53	51	49	47	49	58	43	47	47	51	52	50	41	37	51		
11-	45	51	48	53	42	45	53	53	49	41	48	45	52	45	51	50	49	49	55	43	40	52	53	48	48	52	51		
12-	54	47	44	49	57	49	50	54	54	43	38	51	46	51	52	47	42	50	49	49	48	45	49	53	42	45	51		
13-	53	57	56	54	50	50	56	57	52	55	54	50	59	52	50	50	56	61	55	51	52	58	48	55	57	52	51		
14-	47	42	53	54	49	45	44	49	51	47	50	43	46	45	48	58	47	48	47	52	43	46	54	50	50	49	51		
15-	46	50	49	54	58	57	62	53	52	63	49	44	54	59	49	55	64	52	49	61	54	40	58	51	55	63	51		
16-	49	45	46	49	52	44	48	50	46	53	53	44	41	48	53	50	48	51	50	41	40	54	51	51	51	51	51		
17-	54	48	49	55	44	43	48	43	47	55	48	48	52	44	47	50	49	52	44	53	54	43	50	54	43	41	51		
18-	44	46	53	48	52	47	51	41	54	49	52	48	44	56	50	40	43	53	45	54	49	47	49	52	44	49	51		
19-	39	51	57	47	50	52	43	34	50	51	52	55	47	46	48	43	52	48	51	46	49	60	44	46	45	54	51		
20-	44	40	38	47	39	45	43	41	36	43	43	39	51	4	46	47	39	36	47	36	43	45	47	47	42	50	51		

TOP SECRET ULTRA

6. h-q HAMBURG-TANZANIA

In May, 1943, another circuit was found which exhibited the characteristics of the "Janowski" system employed by Hamburg. This circuit, however, did not use just the fifth group as an indicator, but the first five groups contained the complete enciphered preamble. The traffic was tried for a twenty-length key, and solution was attained with this length. By the time that circuit h-q was intercepted, a further I.B.N. run had been developed, as an aid in solution, making the choice of generatrices more simple.

When the substitution key for the month had been solved (the substitution key was constant for a month), it was then possible to vary the procedure described under circuit h-p so that the correct totals would always appear in a diagonal line when the tabulation was run off. It was only necessary to take the I.B.N. cards representing the cipher text in the assumed column lengths in the order of the known substitution key (see Figure 17). For example, with the solved key

6 - 9 - 8 - 18 - 5 - 14 - 4 - 13 - 20 etc.

we take the cards for column 6 (in Figure 18 this would be D, H, H, M, G, U, and a separator card), then column 9 (Q, W, C, Y, P, K, and a separator card) etc. When the cards are run off, an examination of the highest totals shows a diagonal line starting at generatrix 15, continuing through generatrix 26, starting again at generatrix 1, continuing through generatrix 8. This leaves the six unused generatrices in positions 9 through 14. Generatrix 15 will then be found for column 6 (See figure 18) as

R
V
V
A
U
I

Generatrix 16 will apply for column 9, etc. The reference letter used for this particular encipherment can be found by placing the six unused letters of the sliding alphabet under the known unused letters (U through Z) of the stationary alphabet and reading the letter A. Thus, in this case letters 9 through 14, or I through N, are unused:

TOP SECRET. ULTRA

FIGURE 17

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Solved	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Key	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
6--35	37	27	28	27	35	34	34	33	24	34	36	31	31	31	34	23	34	29	29	35	34	29	31	36	34	35
9--24	31	34	35	36	32	31	31	32	31	35	31	33	31	31	31	31	35	35	32	30	28	35	32	34	36	29
8--36	28	25	35	30	33	37	38	28	26	38	36	30	33	32	32	25	37	28	31	30	34	33	32	36	31	34
18--36	35	35	24	30	35	32	32	32	31	30	33	33	31	33	33	30	33	38	26	32	35	30	23	34	36	33
5--32	32	31	33	35	36	33	35	38	23	27	35	31	32	35	33	25	33	38	35	29	32	33	32	28	28	
14--35	30	36	31	32	29	32	35	32	30	32	30	37	28	31	33	35	33	34	32	29	34	32	30	25	33	
4--34	34	29	35	38	31	30	35	35	29	26	33	33	36	32	32	25	31	36	36	32	28	29	31	29	28	
13--26	26	36	34	36	36	31	25	35	33	31	36	28	30	33	30	33	32	34	30	32	32	30	33	35	31	
20--31	32	32	32	29	32	35	30	26	33	34	31	36	36	31	33	31	30	33	27	31	31	37	37	33	32	
1--37	33	35	32	38	30	33	32	35	28	30	34	30	40	31	30	24	36	37	35	31	26	35	36	23	29	
17--35	36	30	23	34	30	31	38	32	28	29	33	34	37	30	31	31	32	27	33	38	34	30	31	32	31	
16--34	33	35	36	27	35	33	32	31	32	34	33	28	28	32	32	36	35	35	25	33	32	31	28	31	35	
3--37	25	26	33	33	32	37	34	25	29	36	36	33	28	30	34	29	26	33	33	34	35	38	38	29	33	
12--31	38	37	31	26	35	32	28	30	31	33	36	29	33	33	34	36	32	34	28	32	36	33	27	28	30	
2--34	32	32	29	31	36	27	25	34	32	32	36	37	35	27	36	36	29	30	33	29	32	33	31	28	32	
15--33	33	30	34	32	27	36	35	29	31	38	31	31	36	33	29	32	28	30	37	31	32	31	28	34	36	
7--32	35	31	34	32	28	30	34	34	26	34	33	26	35	35	33	29	30	32	36	28	27	33	37	27	33	
10--34	30	31	27	32	36	34	32	28	34	39	24	31	31	34	33	30	36	29	35	36	32	25	32	34	35	
19--30	32	31	33	34	32	34	30	35	32	31	32	33	32	34	38	29	30	29	34	30	35	34	29	35	27	
11--37	35	35	31	29	22	31	36	36	34	31	34	30	27	34	36	31	28	34	38	31	35	35	27	24	34	

FIGURE 20

120

TOP SECRET USTRA

FIGURE 15 - CONTINUED

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	G	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	M	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

TOP SECRET ULTRA

12 3 4 5 6 7 8 9 D 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

15

16

17

18

19

20

16

17

18

19

20

TOP SECRET MATH

Stationary

N O P Q R S T U V W X Y Z A B C D E F G H I J K L

Slide

B C D E F G H I J K L M N O P Q R S T U V W X Y Z A

M is found to be the reference letter. This method of using the weights greatly expedited solution on this type of problem, particularly when the substitution had once been solved for the month.

7. 4-I HAMBURG-BORDEAUX

All the circuits using the "Janowski" method employed a diagram of twenty letters in width except circuit 4-I. During the period July - November, 1942, this circuit used the "Janowski" method with a key length of sixteen letters, but this fact was not discovered until long after all the details of this method were well-known. In this adaptation of the system, nulls were inserted in the diagram according to the sixteen-letter transposition key for five lines, then reflected for the next five lines. The null letters themselves were from a random selection. The preamble consisted of the first five groups, the first four groups containing the usual preamble, and the fifth group serving as a check on the enciphering date. The fifth group key was different from the key used in the first four groups, i.e.,

1 2 3 4 5 6 7 8 9 0
L K J I H G F E D C

This method continued until the middle of November, 1942, at which time this circuit changed to the type system previously described under E-2. However, this case is the only one known to this office in which nulls were used with the "Janowski" system.

In April, 1943, circuit 4-I changed systems again. Their return to the use of "Janowski" type was discovered by the British. During the life of this system (April and May, 1943) the key employed was a 22-length instead of the usual 20-length key. Much of the traffic was read, and on one occasion it was found that the deciphered message proved to be a transposition message, obviously a relay. With this fact in mind, it became possible to solve a Janowski key for two previously unsolved messages, both of which were cipher relays of transposition messages.

Several months later these three transposition messages were identified definitely as messages originally transmitted on a

TOP SECRET ULTRA

different circuit. Their identification was one of the factors which led eventually to the solution of later Enigma traffic on this circuit.

F. DOUBLE TRANSPOSITION

1. 4-O BERLIN-MADRID

This was the first double transposition circuit to be solved by the Coast Guard. Traffic was first intercepted in late 1942, and it soon became obvious that the first two and last two groups of each message were a dual encipherment of the indicator. By means of a normal alphabet with variants (starting with W) these indicators deciphered into numbers as follows:

- (a) The first 5 digits ranged under 400, indicating the pages of a book.
- (b) The next 2 digits ranged low enough to indicate a line number.
- (c) The next 4 digits ranged (for each pair) from 10 to 30.
- (d) The last digit was not significant.

It seemed obvious that the only use to which the pair of numbers between 10 and 30 could be put as indicators would be to designate the number of letters selected from the line indicated. Since there were two such selections indicated, a double transposition system seemed the obvious conclusion. Accordingly, a search was made for the classic case of the double transposition being nullified by the length of the message being equal to the product of the widths of the two keys. A few such cases were found and easily anagrammed for solution, thus verifying the assumed derivation of keys and the use of the indicators. Upon recovery of the literal keys, it was found that the two keys read in sequence.

The next successful solution on this traffic involved cases of the length being multiple of the product of the two widths which is, if anything, an easier solution than the aforementioned one.

Another type of successful solution resulted in the case where the length was one and one-half times the product of the two widths. In these cases, any time two adjacent numbers in the first transposition key differed by a multiple of 2 it would be possible to align the corresponding rows and one-half of adjacent rows from the second diagram. Success was also achieved with cases where the part factor constituted one and one-third, one and two-thirds, and the like.

TOP SECRET ULTRA

A message transmitted on 26 December, 1942 from Madrid to Berlin presented the most interesting case of the product plus a fraction solved in the 4-O traffic.

The message contained 147 groups after the 4 indicator groups were removed. The widths as given in the indicator were 21 in both transpositions. Thus with a message length of 735 letters both diagrams were completely filled with a width of 21 and a depth of 35 letters.

By writing the cipher text vertically in a width of 21 (Fig. 19), it was noted, after marking the column splits from the first transposition, that a full cycle was completed after each 3 lines of the first transposition.

TOP SECRET ULTRA

FIGURE 10

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1-2	X	E	R	E	E	S	N	O	N	G	D	R	T	E	A	I	N	E	E	E	E
2-3	T	O	C	S	A	R	T	I	E	N	E	Q	P	C	L	A	S	O	I	K	C
3-4	A	N	G	X	A	N	E	I	E	R	X	E	I	J	O	T	S	N	N	E	N
4-5	Z	S	M	E	D	S	I	X	A	R	T	N	U	V	E	N	F	V	E	X	E
5-6	S	M	E	D	S	I	X	A	R	T	N	U	V	E	N	F	V	E	X	E	X
6-7	S	M	E	D	S	I	X	A	R	T	N	U	V	E	N	F	V	E	X	E	X
7-8	S	M	E	D	S	I	X	A	R	T	N	U	V	E	N	F	V	E	X	E	X
8-9	S	M	E	D	S	I	X	A	R	T	N	U	V	E	N	F	V	E	X	E	X
9-10	S	M	E	D	S	I	X	A	R	T	N	U	V	E	N	F	V	E	X	E	X
10-11	S	M	E	D	S	I	X	A	R	T	N	U	V	E	N	F	V	E	X	E	X
11-12	S	M	E	D	S	I	X	A	R	T	N	U	V	E	N	F	V	E	X	E	X
12-13	S	M	E	D	S	I	X	A	R	T	N	U	V	E	N	F	V	E	X	E	X
13-14	S	M	E	D	S	I	X	A	R	T	N	U	V	E	N	F	V	E	X	E	X
14-15	S	M	E	D	S	I	X	A	R	T	N	U	V	E	N	F	V	E	X	E	X
15-16	S	M	E	D	S	I	X	A	R	T	N	U	V	E	N	F	V	E	X	E	X
16-17	S	M	E	D	S	I	X	A	R	T	N	U	V	E	N	F	V	E	X	E	X
17-18	S	M	E	D	S	I	X	A	R	T	N	U	V	E	N	F	V	E	X	E	X
18-19	S	M	E	D	S	I	X	A	R	T	N	U	V	E	N	F	V	E	X	E	X
19-20	S	M	E	D	S	I	X	A	R	T	N	U	V	E	N	F	V	E	X	E	X
20-21	S	M	E	D	S	I	X	A	R	T	N	U	V	E	N	F	V	E	X	E	X
21	S	M	E	D	S	I	X	A	R	T	N	U	V	E	N	F	V	E	X	E	X

Column 1 could match with columns 4 or 7 if either of those columns were adjacent in the first transposition. By the same token 14 and 17 could match. If columns 1 and 4 are adjoining in the first transposition key, the horizontal lines 1 and 4 would yield 21 correct digraphs. Simultaneously the line marked 1 and 2 would match with line 4 and 5 producing 14 correct digraphs of the 21 derived. The seven wrong digraphs are then the product of the last 7 columns (15-21) in the second transposition.

A further pairing (columns 14 and 17) would mean horizontal lines 14 and 17 would produce 21 correct digraphs. Lines 15-16 and 16-17 would produce 7 right digraphs out of 21. This provides a further check on the paired letters between 1-2 and 4-5. Those combinations which were wrong in the 1-4 pairing would be correct in the 14-17 lines: i.e., the right seven in 14-17 would be in columns 15-21 of the second transposition figure:

	15,1,4	15,1,4	10,7	10,7
1	X X N	N T Z	A E	R D
2	V E G	E X U	D A	A L
3	E R A	N E N	O R	T X
4	D E R	I S T	O P	I C
5	B E I	I N X	F T	R N
6	E S E	C H B	S Z	O F
7	C N Q	N U C	Z U	A D
8	L O C	N D K	N U	T I
9	X B E	E T A	B W	T E
10	A C H	E D V	D E	R A
11	E N K	A G I	E N	E S
12	L Z W	D E S	T D	E N
13	A X D	U T O	T T	S T
14	G N E	E N D	N I	R A
15	C H E	E D A	I E	E O
16	D A S	E I G	N I	N A
17	E N S	I E S	R S	U N
18	L T E	N D E	I S	S I
19	T R A	B E T	S E	O O
20	I E D	M K R	I S	N E
21	R A E	I N X	O S	L I

7 wrong

7 wrong

TOP SECRET ULTRA

14 17
N X
T I
F R
N E
E I
E U
Q Q
E D
D I
A N
B R
P A
G E
I L
X N
D A
E I
N X
S U

14 17
N J
E W
N E
I K
I M
C X
N G
N I
E E
E S
A N
D C
U T
E X
E I
E D
I N
N D
B T
W E
I I

14 17
A B
N H
V O
H E
I K
U G
E K
I R
S I
E M
N I
A R
E G
E N
E N
T R
S X
A M
I O
S O
E E

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

Of these,
the last
7 are right.

Of these,
the first
7 are right.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

3 18 9
A L X
N T P
X X J
A R S
E I S
I T B
R H E
G R U
I N D
I C H
E R V
C K T
N I B
T E S
N I M
X Q Q
R I E
U N G
N I O
N T I
L I C

3 18 9
T B I
C H I
G O I
S E A
N K U
I G T
E K R
T R E
D I E
A M M
R I E
A R S
M G I
I N T
A N K
E R S
E X E
U M S
I C M
N O Z
H E N

Of these, 14 are right.

TOP SECRET ULTRA

The column arrangement as shown is not the true key. Each unit of 7 columns is in the correct segment.

The first 147 letters of the plain text may now be selected.

1	2	3	4	5	6	7	8	9	0	1	1	1	1	1	1	1	2	2
X	X	N	H	U	P	E	L	U	A	A	E	X	E	X	C	N	K	P
R	U	I	A	C	O	R	D	T	G	A	S	E	N	U	X	C	G	N
E	D	R	R	K	E	P	I	E	O	T	N	D	N	P	I	I	G	E
B	D	I	E	V	I	W	A	T	B	R	N	X	E	X	S	N	H	I
Z	D	E	W	A	H	D	O	S	T	E	E	L	E	T	N	I	R	S
X	D	N	D	E	X	T	I	Z	T	S	N	A	N	S	R	D	O	P
N	E	N	S	T	R	S	G	N	R	O	S	E	B	E	G	T	E	R
N	U																	

15	14	10	7	14	17	3	18	9	2	20
X	X	A	E	E	N	N	K	U	X	X
E	R	A	G	R	N	G	I	O	T	U
D	E	R	O	P	N	I	R	I	E	D
X	B	E	B	W	E	S	I	N	T	D
L	Z	W	T	D	E	I	E	R	S	D
A	X	D	T	T	N	D	N	O	Z	D
E	N	S	R	S	B	T	H	E	N	E

A.

13	14	10	7	16	19	
X	X	A	E	C	F	1
E	R	A	G	X	N	2
D	E	R	O	P	G	3
X	B	E	B	W	N	4
L	Z	W	T	D	S	5
A	X	D	T	T	P	6
E	N	S	R	S	R	7

B.

2	20	14	17	5	8	11
X	X	E	N	U	L	A
U	T	N	O	C	D	A
D	E	N	I	K	I	T
D	I	E	S	V	A	R
D	I	E	I	A	O	E
D	E	N	D	E	I	S
E	N	B	T	T	G	O

TOP SECRET ULTRA

5 18 9	6	12	15	21
N K U	P	E	X	T
I G T	O	S	U	E
R I E	E	N	N	A
J N T	I	N	E	A
E R S	H	E	T	D
N O Z	X	M	S	G
H E N	R	S	E	U

The known correct matches in the first transposition are noted and a further anagramming is now necessary to complete the solution.

Columns 5-18-9 seem the easiest point to begin. The trigraph NOZ suggests the proper name MUNOK. HEN suggests ANKUNFT. Column 6 could easily match with columns 5-18-9, one column separating them, as follows:

5189 6
NKUP
IGTO
RIEE
INTI
ERSH
NOZX
HENR

We now examine the remaining single columns in A and B for a column containing an N for ANKUNFT; a C for the SCH combination; an X for the punctuation after MUNOK, and possibly a G to end the trigraph RIE. Only column 16 of the A group meets these requirements. The letters are rearranged into the diagram and all of the A group is thus rearranged.

1 1	1	10 7	19	12	15	21
5 8 9 6 6	3 1 4	T D	S	E	X	T
NKUNFP	LZW	B W	H	S	U	E
IGTXO	XDE	R S	R	N	N	A
RIEGE	ENS	T T	P	N	E	A
INTRI	AXD	A E	F	E	T	D
ERSCH	XXH	G R	N	M	S	G
NOZX X	ERA	O P	G	S	E	U
HENPR	DER					

TOP SECRET ULTRA

Columns 10-7 could well follow column 6 as follows.

```

1 1 1
S S S S S
N K N P T D
I G T X O B W
R I E G E R S
I N T R I T T
E R S C H A E
N O Z X X G R
H E N P R O P
    
```

If we are able to rearrange columns in section 3 the anagram can be readily completed. A rearrangement of Column 5 in Section 3 will produce the desired letters to precede Column 3. Section 3 may now be arranged in entirety.

```

1 1 1
S S S S S 15 14 19 12 15 21 2 20 14 17 8 11
A N K U N P T D L Z W S E X T D I E I O E
T I O T X O B W X B E H S U E C N B T O O
K R I E G E R S E N S R N N A D E N D I T
E I N T R I T T A X D P N E A D E N D I S
V E R S C H A E X X N F E T D D I E S A R
U N O Z X X G R E R A N N S G X X E N L A
C H E N P R O P D E R O S E U U T N G D A
    
```

The complete first transposition may be recovered at this point.

```

2 1 1 1 1 2 1 1 1 1 1 1
1 4 7 3 1 4 8 5 2 0 2 5 3 8 9 6 6 0 7 1 9
T E I L Z W O X D I E A N K U N P T D E S
E B T X E G U E N S T I G T X O B W O H
A N I E N S I N D E N K R I E G E R S T R
A N D A X D I E D E N E I N T R I T T S P
D E S X X N A T D I E V E R S C H A E R F
G E N E R A L S X X N U N O Z X X G R A N
U N G D E R D E U T S C H E N P R O P A G
    
```

The second transposition key is recovered by rearranging the above 7 lines of text as follows.

TOP SECRET ULTRA

TEILZWOXDIRANKUMFTDES
 GENERALSXXMUNOZXIGRAN
 DESXXNATDIEVERSCHAERF
 UNODERDEUTSCHENPROPAG
 ANDAXDIEDENEINTRITTS
 ANIENSINDENKRIEGERSTR
 EBTXBEGUEWSTIGTXBWOH

This now permits the recovery of the second transposition and the entire message may now be read.

Attempts were made to read messages whose lengths were a few letters in excess of the product of the two widths (in which case the anagramming would be progressively staggered on a diagonal) but the only success attained with such a case was by means of the true general solution for double transposition. In this case, the beginning of the message was correctly cribbed in, and the Railback technique applied from this start.

Since the second literal key was a continuation of the first, it was sometimes possible to read additional traffic by means of expanding the keys first recovered into their longer version when later used. However, a relatively small portion of this traffic was solved. It was noted that, in this circuit some care had been exercised to avoid the cases which would be favorable to solution by the means described herein. In fact, the number of cases where the first enciphering rectangle was completely filled—thus allowing the possibility of columns therefrom to be inscribed in phase with each other in the second rectangle—were relatively few.

Eventually, the indicator was reduced to one numerical group representing (it was believed by the British) the number of the page in the first 3 digits and the number of the line in the last 2 digits; to this was added by non-carrying addition a constant 5 digit group. From the line so determined were selected the first 4 words for the first key and the first 4 words from the line following for the second key. An absolute solution for the constant additive was never obtained, and so no traffic in the newer system was read.

TOP SECRET - TMA

2. h-0 BEHLEN-TETUAN

When the first intercepts were made on this circuit, the indicator system used was of the type first employed by the Germans for double transposition, i.e., the indicator gave only the date of encipherment. This was done in a peculiar manner: the control station had a four digit group in the preamble, the middle two figures of which gave the day of the month, and the middle two gave the date in the last group of the month, and the answer station letter equivalents for the figures according to the table:

1	2	3	4	5	6	7	8	9	0
A	D	O	K	N	Q	T	V	X	Z
B	E	H	L	O	R	U	W	Y	
C	F	I	M	P	S				

The middle letter of the group was a null. The first and second letters gave the day of the month, which was repeated with different letters in the fourth and fifth places.

Very little traffic was intercepted while the circuit was using this system and no solution was achieved by this office. A description of the keying system and a list of keys was received from the British. From this it was learned that the first decipher key was determined by the day of the week; i.e., there were only seven such keys; and the second decipher key remained constant for one week.

This circuit changed their system on April 1, 1943 to one similar to that first used by h-0, and described under that heading. Since this type of indicator system was already known, the letter-equivalents for the digits were quickly solved, but, unlike h-0, proved to be derived from a key word mixed sequence.

1	2	3	4	5	6	7	8	9	0
U	E	B	I	M	R	T	N	D	L
C	H	K	A	F	G	J	O	P	Q
S	V	W	X	Y	Z				

* Some months later attention was directed in another system to a German proverb used as a key, and it was observed that the above key could be constructed from the same proverb --
UEB DAGER TREU UND REDLICHKEIT.

TOP SECRET. ULTRA

After this solution of the indicators, it was a simple matter to pick out favorable cases like those used to break 4-O messages. Many such cases were found and successfully anagrammed.

The cryptographers on this circuit were particularly careless. They were addicted to the use of a completely-filled first enciphering rectangle, so that the number of favorable cases were correspondingly greater than normal. In addition to this, they chose most of their keys from the top ten lines of the page, with the very first line being a particular favorite, and with the same keys were repeated time and again. This enabled many unique solutions to be made when literal keys had been derived. In some cases successful solutions were achieved without the literal key, by expanding or contracting numerical keys previously used to the lengths designated for the message under study.

The circuit changed November 4, 1943, to the same type of numerical indicator as 4-O, and solutions ceased. The British had solved other circuits using this type of indicator and in all such cases the key book was not changed, so it was assumed that this circuit was continuing to use the old key book. This was at least partially confirmed by the work done in trying to solve the additive (non carry-over) that had been used. It was possible to get fairly certain values for four figures of this additive, (the first, second, fourth, and fifth digits) by assuming the page number was never higher than 240 and the line number never higher than 26. There were no contradictions found on this theory, but it was not possible to fix the third digit of the additive, since there were no limitations on the plain digits that could occur in this place. Attempts were made to go through the laborious process of assuming all ten possible digits in this place, in succession, searching for a key previously used, which, if our assumption were correct, would give us the second encipher key used; by applying this to the cipher text, the message would then be reduced to single transposition, with an unknown key length. This might have yielded results, tedious as it was, and did indeed result in the probable elimination of several digits for this place - but in the meantime, traffic from this circuit ceased.

The book used by this circuit to derive their keys was approximately 240 pages in length with no more than 26 lines to the page. It was obviously a translation into German of some detective story originally written in English, but despite intensive efforts by our office and by the British, it was never located.

3. 4-0 ENIGMA-TRAFFIC

This traffic was believed from the first to be double transposition, but there was no verification of this belief for some time. The only apparent indicators were the dates, which were sent unenciphered in the preamble, and a number, which was also sent in the preamble like a message serial number, but which did not run in sequence as would be expected of serial numbers. Attempts to apply the solution techniques used in the 4-0 and 4-5 to possibly favorable cases were unavailing.

One instance occurred, which suggested that double transposition was employed. A message ("25 GR 1006/146") was corrected and retransmitted ("25 GR 1006/173") and, upon examination, the two versions proved to contain identical sections of cipher text, but in different permutations. These sections were 16 in number of only 2 lengths (7 and 8 letters), and comprised the entire message (thereby eliminating the likelihood of an enciphered indicator). When written out on a width of 16, the matches in the position of the columns between the corrected version and the first version was as follows:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
15	6	2	10	16	5	14	3	7	13	8	11	1	4	9	12

It was impossible to anagram the columns to produce plain text.

Later there occurred a situation which provided an intriguing modification of a familiar text-book solution. Again a message ("24 GR 178/0609") was corrected and retransmitted. In this case, it was first noted that the first three letters of each version were identical and that similar three-and four-letter identities occurred elsewhere in identical positions in the two versions; however, these were not symmetrically distributed through the cipher text, as is the normal situation for a significant repeat which has undergone a columnar transposition (i.e., the repeat, if significant, must extend over several complete rows of the diagram and must therefore be represented in every column after transposition). Here it was considered that the message might have been paraphrased before re-encipherment; however, a frequency count of the two versions established, with reasonable certainty, that — allowing for a few garbles — the two versions contained identical plain text.

The subdivision of the cipher text into correct long and short

TOP SECRET ULTRA

column was made possible solely on the basis of the hypothesis that there must always be an identity (of no less than 2 letters since most of them were 3 letters) at the top of each column and for one letter at the bottom of every long column. (Allowance for garbles was made in case of the last letter of columns 17 and 18.) The diagram shows the columns of the two versions divided into sections according to the matches between the columns. That is, Section I, III and V corresponded by columns as shown in the sequence of numbers in parentheses above Section I; Section II corresponded as shown in the sequence immediately above it; Section IV (as may be seen) showed some apparent matches, but they proved to be neither easily determinable nor necessary to solution of this message.

Considering, now, the comparison of the two versions of this message, it was evident that the two second keys could be established simply by rearranging the divided columns so that the outline of each section became continuous instead of intermittent, line by line. It was thus possible to determine the following facts about the two second keys:

A. Corrected Version:

- (1) From Section V, columns 3, 10 and 11 must be in positions 18-20.
- (2) From Section I, columns 2, 3, 10, 11 and 16 must be in positions 16-20; therefore, columns 2 and 16 must be in positions 16 and 17.
- (3) From Section IV, columns 2, 3, 7, 10 and 11 should be in positions 16-20; but column 7 is long and therefore cannot be in the last 10 positions; therefore, columns 2, 3, 10 and 11 must be in positions 17-20; therefore, column 16 is in position 16 and column 2 is in position 17.

B. Original Version:

- (1) From Section V, column 3, 9 and 11 must be in positions 18-20.
- (2) From Section I, columns 2, 3, 9, 11 and 17 must be in positions 16-20; therefore, columns 2 and 17 must be in positions 16 and 17.

- (3) From Section IV, columns 2, 3, 9, 11 and 12 should be in positions 16-20; but column 12 is long and therefore cannot be in the last 10 positions; therefore columns 2, 3, 9, and 11 must be in positions 17-20; therefore column 17 is in position 16 and column 2 is in position 17.

These determinations produce the following alignments:

A. Corrected Version:

Pos. 16 17

Key 16 2

Sect. I 17 2
T A

13 1

Sect. II L R
I Q
S U
N R
M

B. Original Version:

Pos. 16 17

Key 17 2

Sect. I 16 2
T A

7 4

Sect. II X L
P L
B R
Q U
K

A. Corrected Version:

Sect. III N N
I E
L X
E Y

Sect. IV N
U E
U L

B. Original Version:

Sect. III N N
I R
I X
L X
E

Sect. IV S T
R A

The similar identities in Section II of the corrected version (i.e. "13/1") indicated that these two columns must have been adjacent in the original version to produce the same portion of Section II in that version; this alignment of columns indicated another portion of Section I which could be aligned in the

TOP SECRET LTR

corrected version; again a portion of alignment of Section II of the original version was indicated; etc. Continuation of this process developed both keys simultaneously, as follows (A represents the corrected version, B the original version; numerals represent sections in which the correspondences occurred. The development progresses down the columns):

A	16	2																
A I	17	2																
A II	13	1	1	14	14	15	15	20	20	6	6	12	12	10				
B I	13	1	1	14	14	15	15	20	20	12	12	7	7	4				
A II	10	7	7	16	16	19	19	4	4	8	8	17	17	2				
B I	4	8	8	18	18	19	19	5	5	9	9	16	16	2				
A II	2	9	9	3	3	11	11	5	5	18	18	13	13	1				
B I	2	10	10	3	3	11	11	6	6	17	17	13	13	1				
	etc.																	

This development obviously gave the relative alignment of all columns of both keys—subject only to the originally determined location of 2 columns in each.

TOP SECRET ULTRA

The second transposition was that derived from each version

A.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	522	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545	546	547	548	549	550	551	552	553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571	572	573	574	575	576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593	594	595	596	597	598	599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623	624	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	649	650	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675	676	677	678	679	680	681	682	683	684	685	686	687	688	689	690	691	692	693	694	695	696	697	698	699	700	701	702	703	704	705	706	707	708	709	710	711	712	713	714	715	716	717	718	719	720	721	722	723	724	725	726	727	728	729	730	731	732	733	734	735	736	737	738	739	740	741	742	743	744	745	746	747	748	749	750	751	752	753	754	755	756	757	758	759	760	761	762	763	764	765	766	767	768	769	770	771	772	773	774	775	776	777	778	779	780	781	782	783	784	785	786	787	788	789	790	791	792	793	794	795	796	797	798	799	800	801	802	803	804	805	806	807	808	809	810	811	812	813	814	815	816	817	818	819	820	821	822	823	824	825	826	827	828	829	830	831	832	833	834	835	836	837	838	839	840	841	842	843	844	845	846	847	848	849	850	851	852	853	854	855	856	857	858	859	860	861	862	863	864	865	866	867	868	869	870	871	872	873	874	875	876	877	878	879	880	881	882	883	884	885	886	887	888	889	890	891	892	893	894	895	896	897	898	899	900	901	902	903	904	905	906	907	908	909	910	911	912	913	914	915	916	917	918	919	920	921	922	923	924	925	926	927	928	929	930	931	932	933	934	935	936	937	938	939	940	941	942	943	944	945	946	947	948	949	950	951	952	953	954	955	956	957	958	959	960	961	962	963	964	965	966	967	968	969	970	971	972	973	974	975	976	977	978	979	980	981	982	983	984	985	986	987	988	989	990	991	992	993	994	995	996	997	998	999	1000	1001	1002	1003	1004	1005	1006	1007	1008	1009	1010	1011	1012	1013	1014	1015	1016	1017	1018	1019	1020	1021	1022	1023	1024	1025	1026	1027	1028	1029	1030	1031	1032	1033	1034	1035	1036	1037	1038	1039	1040	1041	1042	1043	1044	1045	1046	1047	1048	1049	1050	1051	1052	1053	1054	1055	1056	1057	1058	1059	1060	1061	1062	1063	1064	1065	1066	1067	1068	1069	1070	1071	1072	1073	1074	1075	1076	1077	1078	1079	1080	1081	1082	1083	1084	1085	1086	1087	1088	1089	1090	1091	1092	1093	1094	1095	1096	1097	1098	1099	1100	1101	1102	1103	1104	1105	1106	1107	1108	1109	1110	1111	1112	1113	1114	1115	1116	1117	1118	1119	1120	1121	1122	1123	1124	1125	1126	1127	1128	1129	1130	1131	1132	1133	1134	1135	1136	1137	1138	1139	1140	1141	1142	1143	1144	1145	1146	1147	1148	1149	1150	1151	1152	1153	1154	1155	1156	1157	1158	1159	1160	1161	1162	1163	1164	1165	1166	1167	1168	1169	1170	1171	1172	1173	1174	1175	1176	1177	1178	1179	1180	1181	1182	1183	1184	1185	1186	1187	1188	1189	1190	1191	1192	1193	1194	1195	1196	1197	1198	1199	1200	1201	1202	1203	1204	1205	1206	1207	1208	1209	1210	1211	1212	1213	1214	1215	1216	1217	1218	1219	1220	1221	1222	1223	1224	1225	1226	1227	1228	1229	1230	1231	1232	1233	1234	1235	1236	1237	1238	1239	1240	1241	1242	1243	1244	1245	1246	1247	1248	1249	1250	1251	1252	1253	1254	1255	1256	1257	1258	1259	1260	1261	1262	1263	1264	1265	1266	1267	1268	1269	1270	1271	1272	1273	1274	1275	1276	1277	1278	1279	1280	1281	1282	1283	1284	1285	1286	1287	1288	1289	1290	1291	1292	1293	1294	1295	1296	1297	1298	1299	1300	1301	1302	1303	1304	1305	1306	1307	1308	1309	1310	1311	1312	1313	1314	1315	1316	1317	1318	1319	1320	1321	1322	1323	1324	1325	1326	1327	1328	1329	1330	1331	1332	1333	1334	1335	1336	1337	1338	1339	1340	1341	1342	1343	1344	1345	1346	1347	1348	1349	1350	1351	1352	1353	1354	1355	1356	1357	1358	1359	1360	1361	1362	1363	1364	1365	1366	1367	1368	1369	1370	1371	1372	1373	1374	1375	1376	1377	1378	1379	1380	1381	1382	1383	1384	1385	1386	1387	1388	1389	1390	1391	1392	1393	1394	1395	1396	1397	1398	1399	1400	1401	1402	1403	1404	1405	1406	1407	1408	1409	1410	1411	1412	1413	1414	1415	1416	1417	1418	1419	1420	1421	1422	1423	1424	1425	1426	1427	1428	1429	1430	1431	1432	1433	1434	1435	1436	1437	1438	1439	1440	1441	1442	1443	1444	1445	1446	1447	1448	1449	1450	1451	1452	1453	1454	1455	1456	1457	1458	1459	1460	1461	1462	1463	1464	1465	1466	1467	1468	1469	1470	1471	1472	1473	1474	1475	1476	1477	1478	1479	1480	1481	1482	1483	1484	14
--	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	----

TOP SECRET ULTRA

similar, respectively, to their second keys. It was then a simple matter to anagram the plain text for each version.

The two pairs of numerical keys which resulted from this solution were as follows:

Corrected Version:

1st: 17 4 6 14 2 7 3 11 8 18 13 11 15 16 20 12
2nd: 6 17 13 1 14 15 20 12 7 4 8 18 19 5 9 16 2 10 3 11

Original Version:

1st: 18 4 5 14 2 6 3 11 7 19 13 1 15 16 20 8 12 10 9 17
2nd: 5 18 13 1 14 15 20 6 12 10 7 16 19 4 8 17 2 9 3 11

An assumed literal key was recovered for the first key of the corrected version:

R D E N B E C K E R M A N N S L E D E R

and it was discovered that the second key was derived by starting the literal key with the 9th letter and transferring the first 8 letters to the end:

E R M A N N S L E D E R R D E N B E C K

However, no satisfactory literal key could be derived for the original version which had, it seemed obvious now, used the wrong five letters at the end of the key. A pronounceable literal key which would conform to these circumstances was:

R D E N B E C K E R M A N N S E L F E N

At this point, attention was again directed to the case of the message previously referred to of 10 June. In the light of the manipulation of the literal key and successful technique employed in the solution of the September message, an attempt was started to develop the two different keys simultaneously. Considering again the correspondence between the 2 keys:

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
15 6 2 10 16 5 14 3 7 13 8 11 1 4 9 12

TOP SECRET ULTRA

These pairs were "chained" to produce the two equal length cyclic sequences: 1 15 9 7 14 4 10 13 and 2 6 5 16 12 11 8 3. It was noted that, when the three short columns of each message were grouped together:

1 11 15
15 8 9

two pairs from one of these claims necessarily had to occupy two of the three short column positions. This fact indicated that the relationship between the two versions of the second key was merely a cyclic displacement of two positions in either possible direction. Thus, by rearranging the pairs of numbers in either possible direction, the key so that the order of the two cyclic sequences was retained in alternating positions, two possibilities resulted for the two versions of the key:

(A) 8 9 3 7 2 14 6 4 5 10 16 13 12 1 11 15
3 7 2 14 6 4 5 10 16 13 12 1 11 15 8 9

(B) 12 13 16 10 5 4 6 14 2 7 3 9 8 15 11 1
11 1 12 13 16 10 5 4 6 14 2 7 3 9 8 15

It would have been relatively simple to experiment with each of these possibilities; but, with the manipulation of the September key still fresh in mind, the last 8 numbers of each of the possibilities for the second key were placed at the beginning—in order to get an idea of which numerical sequence might more probably have been derived from a literal key. Case B (above), when located in this manner gave the sequence

2 7 3 9 8 15 11 1 12 13 16 10 5 4 6 14,

which was recognized as a shorter version of the correct first key for the September message 17 4 6 14 2 7 3 11 8 18 13 1 15 16 20 12 9 5 10 19. This recognition thereby determined not only the two versions of the second key, but the first key as well. The literal key for this day's message was thus derived (from the previously assumed literal key) as:

BECKERMANNSLEDER

It was not until the capture, in the fall of 1943, of Franz Mayr in Teheran, and the subsequent forwarding to this office of the A.A.F.I.W.E. file on his interrogation that the remainder of the traffic on this circuit could be read. The details of the

TOP SECRET ULTRA

system for deriving the keys (which was disclosed by Ma/r) were as follows: The complete literal key was a six line verse:

DER WART ES RITTERSHAN ODER KNAPP

ZU TAUCHEN IN DIESEN SCHLUND?

EINER GOLDENEN BECHER WERF ICH HINAB

TE SCHLÄNGEN SCHON HAT IHN DER SCHWARZE MUND

DER NUR DEN BECHER KANN WIEDER ZEIGEN

ER HAT IHN BEHALTEN ER IST SEIN EIGEN

(The underlined portion is that involved in the two messages which were solved)

The month determined the pair of lines from which the numerical key was derived; the day of the month determined the number of the letter in this pair of lines with which the literal key was started; the month then determined the minimum number of letters taken from this point; and the month finally determined the number of letters which were transposed from the beginning to the end of the first key in deriving the second key. The elements which varied according to the month were controlled according to the following table:

	Jan.	Feb.	Mar.
	Apr.	May	June
	July	Aug.	Sept.
	Oct.	Nov.	Dec.
Lines	1-2	3-4	5-6
Min. Length	14	15	16
Transposition of Key	6	7	8

Concerning the minimum length: If, after taking the minimum number of letters, the end of a word had not been reached, the word was completed. It was this fact which, more than any other, interfered with the solution of additional messages transmitted at times near the dates of the two which were solved. Had this

TOP SECRET ULTRA

procedure not been introduced, it is believed that the erroneous recovery of the literal key would not have stood in the way of additional solutions — in fact the ZEIGEN which was incorrectly used for the September key would have furnished several correct keys.

TOP SECRET ULTRA

This circuit was actually comprised of several circuits. A number of different transmitting stations are known to have operated, several of them simultaneously, in and around Buenos Aires, and the volume of traffic was of impressive proportions. A variety of systems were simultaneously and successively employed. The only hand-transposition system discussed here. This circuit is the double sample of the cumulative effect of an apparently innocuous blunder.

Transposition traffic was transmitted first in November 1942, but apparently no regular schedules were established until January 1943, at which time the few messages previously intercepted until January repeated without change in preamble or cipher text. This class of messages, like the machine traffic, contained apparent serial numbers in the preambles.

No success was had in attempts to solve messages in this system until a message transmitted on 16 March, 1943, was solved by the British and the keys furnished this office.

The particulars of this message were as follows: The length of the message was 120 letters and the number in the preamble presumably the serial number of the message, was 623. The first enciphering key was a width of 10: 10 2 7 1 5 5 6 8 4 9, and the second enciphering key was a width of 12: 9 2 1 5 10 12 11 7 2 8 4 6. The plain text was, as suspected, German; and it was preceded by 16 low-frequency letters used as nulls and followed by 15 similar low-frequency nulls. Oursory attempts were made to derive literal keys for the numerical keys used; but owing to their brevity, not too keen disappointment was felt when this was fruitless. As anticipated, it was also found that the two keys recovered would not read any other messages.

At this point, attention was again directed to an overall study of the traffic at hand—in the hope of finding additional favorable cases for solution. A very striking phenomenon then became apparent in the following message which was also transmitted on 16 March, 1943, with the preamble number 615, and a group count of 42:

OIXFN JOUS MRUAF XELQN AXDZY
SXXIU LTNLQ ENYUU YTNXH LIXJT
XJNQN XYELB ABXXR NZRTB TEEAN
BLQEZ XASQD XYHAQ WLEIE NRILN

TOP SECRET ULTRA

G	E	O	N	D	X	Q	N	B	Y	C	I	X	B	L	X	A	W	Q	U	E	Q	E	R	Y
L	N	X	C	I	Q	N	T	Q	T	M	N	Q	I	L	Y	N	U	X	X	L	Q	N	O	Y
X	A	V	Q	R	D	Y	S	K	Q	N	L	X	I	O	H	C	T	V	V	Z	O	X	E	C
N	X	W	X	T	X	Y	S	D	Y	E	S	Y	X	L	Q	Z	U	X	E	V	R	P	O	E
E	L	T	C	R	A	H	S	F	U															

It was first observed that, within certain sections of the foregoing cipher text, certain letters (Q and Y which are virtually completely lacking in normal German plain text) recurred in surprising periodicity (cf. the passage: X A W Q U E Q E R Y L N X C I Q H T Q T M N Q I L Y N U X X L Q N O Y). Furthermore, it was found that, by judicious selection of X's, the periodicity in the positions of the nulls could be extended. Remembering the use of nulls at the beginning and end of the message previously read, it was obvious that this was a manifestation of the same procedure.

There were two striking points about the location of these nulls: first, they occurred only within certain segments of the cipher text; second, they occurred in periodic order when present. Only brief consideration was necessary to realize that both these points indicated that the first enciphering rectangle was completely filled. For since the cipher text represents columns transcribed in numerical order from the second enciphering rectangle, the absence of nulls from some columns shows a limitation of the point at which columns from the first enciphering rectangle could begin and end in their horizontal transcription into the second enciphering rectangle. And, since in any column the nulls apparently recurred an equal distance apart vertically in the second rectangle, it is obvious that columns from the first enciphering rectangle could begin and end in the same horizontal position only after a constant number of columns from the first enciphering rectangle had been transcribed in the intervening interval. These two conditions could only be satisfied by all columns of the first enciphering rectangle being equal. (This reasoning is valid only when based on the premise that the nulls were located solely at the beginning and end of the plain text, and the additional premise that the nulls in any column of the second rectangle were all from either the beginning or the end of the first rectangle. Had either or both of these premises been incorrect, it is conceivable that the phenomena might have occurred by chance. However, it is implausible that, under any other circumstances than those assumed, these two points would have been as observed.)

Still more significant is a corollary to the foregoing reasoning. The aforementioned fact that a constant number of columns must intervene, in transcription from the first into the second rectangle,

TOP SECRET ULTRA

between two columns starting in the same horizontal position, indicates that a certain number times the columnar-length of the first rectangle equals another number times the width of the second rectangle. More briefly, therefore, there must be a common factor between the depth of the first rectangle and the width of the second rectangle. This established the additional fact that the second rectangle must be completely filled or exceed a completely filled rectangle by a multiple of the aforesaid common factor.

Returning to the cipher text under consideration, it was found that the most obvious—and actually the only possible way of subdividing the cipher text into component columns of the second rectangle, without disturbing the periodicity of the nulls, was in segments of 15 letters each. (cf. the sections of the message: letters 16-60, 121-165 incl.) From this fact, based on the previous reasoning, it became possible to postulate all the dimensions involved in the double transposition. For, a depth of 15 in the second rectangle indicated that this was also completely filled, and had a width of 14. From the interval between nulls in the cipher text, it therefore required 3×14 , or 42, spaces to contain n columns from the first rectangle. Therefore, n could only be 1, 2, 3, 6, 7, 14, 21, or 42, in which case the width of the first rectangle would be 5, 10, 15, 30, 35, 70, 105, or 210 respectively. Obviously, 10, 15 and 30 are the most plausible widths. A width of 15 would give the classic case (since 15×14 equals 210) and a width of 30 would place nulls in every position of some columns in the second rectangle. Therefore 10 is the most plausible width for the first rectangle.

Based on these postulated dimensions, the following facts would be true for a message of 210 letters. A column from the first rectangle could be transcribed into the second rectangle in either of only 2 positions, the odd-numbered columns (according to the first transposition key) in one position and the even-numbered columns in the other position. Each column from the first rectangle would compromise one full row and half of the succeeding or preceding row of the second rectangle. Therefore, any column of the second rectangle would contain letters from the same row of the odd-numbered columns, according to the first transposition key, and other letters from the same row of the even-numbered columns of the first rectangle. There would be 10 letters from columns of one class (5 from one row and 5 from a row 14 above or below the first row) and 5 letters from columns of the other class (from a row 7 above or below the first row). Finally, any time 2 or more adjacent numbers in the first transposition key were of the same class

TOP SECRET ULTRA

(i.e., odd or even), the letters from these columns could be found on homologous levels in the second rectangle, and these two of the second rectangle could be simultaneously ungrammed to produce segments of the original plain text. (See schematic diagram in figure X1).

Figure X1

Schematic Diagram for Double Transposition of a Message of 210 Letters, Using a 10-Letter First Key and a 14-Letter Second Key:

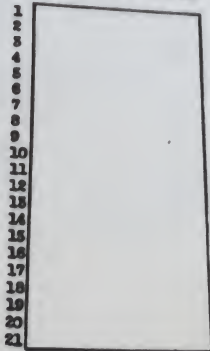
Order of transcribing columns
of the plain text:

Order of columns of the
plain text:

Order of rows of the
plain text:

1 10 8 6 2 3 8 4 7 9 (1st Key)

1 2 5 4 5 6 7 9 9 10



Continued

As columns are transcribed, 2 columns fill 3 rows—placing in any column, letters which come from only 3 rows of the plain text:

Numbers in circles represent the order in which the columns are transcribed from the plain text. Note that the pairs of columns 4 and 5, 7 and 8, and 9 and 10 each start in corresponding positions.

1 2 3 4 5 6 7 8 9 10 11 12 13 14
15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
8 9 10 11 12 13 14 15 16 17 18 19 20 21

Accordingly, the cipher text was written out in horizontal sections of 15 letters, representing the columns from the second rectangle, and numbered to represent the numerical order of columnar transcription from the first rectangle, the middle column of each block of three, below, being made up equally of letters from each of 2 columns of the first rectangle:

1	1	2	3	3	4	5	5	6	7	7	8	9	9	10
or				or		or			or					
2				4		6			8				10	

O	I	X	F	N	J	O	U	U	S	M	R	U	A	F
X	E	L	Q	N	A	X	D	Z	Y	X	X	X	I	U
L	X	N	L	Q	E	N	Y	U	U	Y	T	N	X	H
L	I	X	J	T	X	J	N	Q	N	X	Y	E	L	B
A	B	X	X	R	N	Z	R	T	B	T	E	E	A	N
W	L	E	I	E	N	R	I	L	N	G	E	G	M	D
X	Q	N	B	Y	C	I	X	B	L	X	A	W	Q	U
E	Q	E	R	Y	L	N	X	C	I	Q	H	N	T	Q
M	N	Q	I	L	Y	N	U	X	X	L	Q	N	O	Y
X	A	V	Q	R	D	Y	S	K	Q	N	L	X	I	O
H	C	T	V	V	Z	O	X	E	C	N	X	W	X	T
X	Y	S	D	Y	E	S	Y	X	L	Q	Z	U	X	E
V	E	F	O	E	E	L	T	C	R	A	H	S	F	U

With but little trouble, the foregoing columns were grouped and anagrammed to the following extent (the upper blocks contain segments of either the first or last 14 rows of the plain text; half of the lower blocks contain segments of the first or last 7 rows of the plain text, while the other half is spurious):

<u>7</u>	<u>1</u>	<u>3</u>	<u>5</u>	<u>6</u>	<u>8</u>	<u>4</u>	<u>10</u>	<u>2</u>	<u>2</u>
S	O	F	O	U	R	J	F	X	U
Y	X	Q	X	Z	X	A	U	L	X
U	L	L	N	U	T	E	H	N	N
N	L	J	J	Q	Y	X	B	X	E
B	A	X	Z	T	E	N	N	X	E
D	B	E	A	Q	Y	X	Q	Q	H
N	W	I	R	L	E	N	D	E	G
L	X	B	I	B	A	C	U	N	W
I	E	R	N	C	H	L	T	E	N
X	M	I	N	X	Q	Y	Y	Q	X
Q	X	Q	Y	K	L	D	O	V	N
C	H	V	O	E	X	Z	T	T	W
L	X	D	S	X	Z	E	E	S	U
R	V	O	L	C	H	E	U	F	S

TOP SECRET ULTRA

7	1	8	5
W	W	W	W
Y	Y	Y	Y
X	X	X	X
T	T	T	T
X	X	X	X
Q	Q	Q	Q
L	L	L	L
N	N	N	N
N	N	N	N
Q	Q	Q	Q
A	A	A	A
E	E	E	E
E	E	E	E
T	T	T	T

6	7	5
W	W	W
D	D	D
Y	Y	Y
Y	Y	Y
Y	Y	Y
X	X	X
X	X	X
U	U	U
S	S	S
X	X	X
Y	Y	Y
Y	Y	Y
T	T	T
A	A	A
E	E	E

9	1
W	W
10	10
X	X
X	X
X	X
L	L
L	L
Q	Q
Q	Q
Q	Q
Q	Q
X	X
X	X
X	X
X	X
E	E

9
W
10
X
X
X
L
L
A
A
M
Q
Q
O
O
X
X
X
F

At this point, it appeared that the first key was the same as that for the other message already solved. Accordingly, the foregoing anagrammed portions were written out in the order of the first key, the odd-numbered columns in one group and the even-numbered columns in the other groups:

10 2 7 1 3 5 6 8 4 9

F X	U R J	1
U L	Z X A	2
H N	U T E	3
B X	Q Y X	4
N X	T E N	5
Q Q	Q Y X	6
D E	L E N	7
U N	B A C	8
T E	C H L	9
Y Q	X Q Y	10
O V	K L D	11
T T	E X Z	12
E S	X Z E	13
U Y	C H E	14
X Y	U M M	15
I E	D S N	16
X X	Y Y Q	17
L I	N X T	18
A B	R T F	19
A L	S Y Z	20

10 2 7 1 3 5 6 8 4 9

S O V O	U
X X Q X	X
U L L N	N
N L J J	E
B A X Z	E
D B E A	N
N W I R	G
L X B I	W
T E R N	W T
X M I N	N
Q X Q Y	X
C H V O	W
L X D S	U
R V O L	S
M I N U	Q
S E N D	I
Y X Q Y	X
X I T N	L
T B R R	A
X L E S	A

TOP SECRET ULTRA

M-L	X-C-E	21	O-L-N-I	M
Q-Q	X-Y	22	X-Q-Y-X	Q
Q-Q	G-Q-Y	23	Q-Q-Y-X	Q
Q-Q	U-L-L	24	L-S-L-U	Q
I-A	S-N-R	25	N-A-R-S	I
I-C	X-N-V	26	N-C-V-X	I
I-Y	Y-Q-Y	27	Q-Y-Y-Y	X
Y-E	T-A-E	28	A-S-S-S	F

(The combinations which are crossed off in the lower blocks could be eliminated because the other combinations involving the same line were more obviously segments of plain text.)

At this point, it was not too difficult to superimpose each line from the left on some line from the right, and rearrange the resulting complete lines to produce the complete plain text. In the following diagram, the numbers indicate the lines from the preceding diagram which were combined:

	10	27	1	5	6	8	4	9
19	4	1	A	B	S	O	F	O
20	7	P	E	N	W	I	R	T
18	12	L	I	C	H	V	O	N
24	5	O	N	U	L	N	U	L
20	8	A	L	L	X	B	I	S
11	9	O	V	I	E	R	N	K
2	13	U	L	L	X	D	S	2
1	5	P	X	B	A	X	A	U
7	14	D	E	R	V	O	L	L
12	4	T	T	N	L	J	J	E
5	10	N	N	X	M	I	N	U
8	6	U	N	D	B	E	A	B
9	25	T	E	N	A	R	S	C
13	16	E	S	S	E	N	D	X
5	15	N	I	M	I	N	U	T
14	21	U	F	G	L	E	I	C
4	26	B	I	N	C	V	X	Q
10	17	Y	Q	Y	X	Q	Y	X
6	22	Q	Q	X	Q	Y	X	Q
23	11	Q	Q	X	Q	Y	X	Q
27	2	X	Y	X	Q	X	Y	Q

The correct plain text was as shown in the preceding diagram except that the last two rows of nulls were actually at the beginning of the message; and the actual second key was the vertical sequence of numbers 1 to 14.

TOP SECRET ULYSS

At this point an attempt was made to reconstruct the literal key for this second key: 11 2 1 7 12 3 8 9 13 5 14 4 10 6. Quite obviously, this literal key was found to be as S E C H S E I N S P U S H - the German literal equivalent for the numeral (considered a possible serial number) in the preamble. Returning to the first message solved, the same procedure was found to be true, the literal key was S E C H S E W O D R E I, again the equivalent of the number in the preamble.

Trial of this procedure on other messages established the fact that the first enciphering key was constant and the second enciphering key was always the literal equivalent of the number in the preamble, and it was possible to read all the double transposition traffic transmitted over this circuit. In the process of decrypting back traffic it was found that the first enciphering key had been changed; however, since the second literal key was always provided in the external number, it was merely a routine matter to remove the second transposition and solve the remaining simple columnar transposition.

The literal keys which had been used for the first enciphering transposition were, in chronological order: S O N D E R S C H L U E S S E I, O A S O R S E L L S C H A F T, and S C H A E F F N E R. The latter was the key involved in the two messages originally solved, and from the text was found to be the name of one of the correspondents of this circuit. At about the time these two messages were solved, the Argentina side of the circuit changed its constant key to the correct first and last name of "N O O R D", the cover name for the principal agent in Argentina. This name was never recovered, although its numerical equivalent was easily determined to be: 12 8 6 3 4 10 1 7 2 11 9 5. Contributory evidence later established that NOORD was the agent known as GUSTAV UTZINGER, but the evidence of this key indicates that his true name has never been ascertained, since none of his known aliases would produce this numerical key. During this final period of the double transposition traffic the German side of the circuit retained S C H A E F F N E R as its constant key.

From the foregoing enumeration, it may be seen that the complete solution of the system was considerably facilitated by the original solution of the first message.

It developed, in reading the remainder of the traffic, that, whenever a 2 occurred in the key number in the preamble, it was represented in the literal key by ZWEI. However, in the originally

TOP SECRET U.S. EYES

solved message, it was mistakenly represented as IWO, which fact
shortened the second enciphering key by one number and thus created
a classic cube for solution. Most startling of all was the fact,
disclosed by actual decipherments, that this message, due to this
fact, had never been deciphered by its intended recipient.

TOP SECRET U.S. EYE

DOUBLE TRANSPOSITION-SUBSTITUTION: PLAY-BOOK SYSTEM

6. 1. INTRODUCTORY: CRYPTOGRAPHIC FEATHER OF "ABC SCHLUESSEL"

In the summer of 1943, a new man, *Quartiermeister* Messner of the Cipher Department of the German Army High Command, was given the job of revising and supervising all cipher systems used on the *Heimatschlüssel* circuits. He immediately ordered a revamping of all hand systems then in use, and soon thereafter all *Heimatschlüssel* circuits on the continent and in Africa were observed to change to an entirely new system. In almost every case the control station in *Heimatschlüssel* sent out instructions to the answer station to change immediately to the use of an "ABC SCHLUESSEL". Tests and all methods of attack were applied to the traffic accumulating, but to no avail. It was concluded that the system was apparently some form of substitution-transposition, and that the graphic frequency tables were too flat for monalphabetic substitution, but not flat enough for anything much more complicated. Nothing could be determined as to the complexity of the transposition applied.

At the end of August, the British forwarded a solution of traffic on circuit b-q (*Heimatschlüssel* to *Tangier*). This circuit was, at the time of the change and for some time afterward, sending ten or more messages a day, so that depths up to five were produced. The final complete solution was obtained by working a day's traffic which included a depth of three. (For full details, see "Solution of the 'ABC Schluesel'" in the British publication "Solution of German S.I.S. Hand Ciphers") None of the traffic which led to this solution was available to this office. Later, the British obtained complete details regarding the ABC Schluesel from captured agents and from instructions sent to stations which they controlled.

The system used was, in fact, a combined substitution transposition, as had been surmised.

The substitution was monalphabetic, with the use of variants for the most frequent letters, used in a manner which will be explained later, and the transposition was double columnar transposition. The key for each of the two steps was derived from the same basic key word, but modified in a specific manner for each step, as will be shown later, so that the same two keys for both steps could never be used on different days of the year. The substitution was applied after the text was written into the first rectangle of the transposition, before being transposed into the second rectangle. The

TOP SECRET ULTRA

substitution was made as follows: A cipher alphabet is derived by writing out a given key word, e.g. HIMMELBLAU, without repeated letters, and followed on subsequent lines by the rest of the alphabet in normal sequence, thus:

A	5	7	3	6	2	1	8	
H	I	M	M	E	L	B	A	U
C	D	F	G	J	K	N	O	
P	Q	R	S	T	V	W	X	
Y	Z							

Columns are taken out vertically according to the numerical sequence derived from the key word. This alphabet is juxtaposed against the normal alphabet taking E out of its normal place and inserting it between W and Z when the language used was German and in Spanish A was removed and inserted between V and W. Now the enciphering alphabet, not considering variants, is:

Plain: A B C D F G H I J K L M N O P Q R S T U V W E X Y Z

Cipher: A N W B K V E G S H C P Y I D Q Z L J T M F R U O X

This alphabet was used without change for the first, fifth and ninth lines of the first encipher rectangle. For German, the substitution for the frequent letters E and N would be varied on succeeding lines in the following way: for the second, sixth and tenth lines E would be replaced by U, I by R, N would be replaced by I, and O by Y; on the third, seventh and eleventh lines, E replaced by O, Y by R, N by D and P by Y; on the fourth, eighth, and twelfth lines E replaced by X, Z by R, N by Q, and Q by Y. The substitution alphabets could therefore be expressed as follows:

Plain: A B C D F G H I J K L M N O P Q R S T U V W E X Y Z

Cipher: I	A N W B K V E G S H C P Y I D Q Z L J T M F R U O X
II	I Y D Q U R O X
III	D I Y Q O U R X
IV	Q I D Y X U O R

It is believed from a study of interrogations of captured agents that this is the way the operation was actually performed by the Germans, i.e., as one step for each line.

Exactly the same results could be obtained by considering the substitution process as two separate operations, that is, as the

TOP SECRET U.S.

12	23	1	112	12	22	1	11222	1321
72	19	7	1224	80854	36463	57691	5981003	
S	I	N	O	R	E	I	F	R
A	N	K	E	I	F	R	A	V
O	N	N	I	E	R	A	U	S
K	A							
E	X	I	V	E	R	S	U	C
H	T	E	R	B	I	T	T	E
N	A	N	T	W	O	R	T	H
E	N	N	I					
S	O	M	O	S	A	X	X	S
O	M	O						
S	E	I	N					

The substitution would then be applied, as described above.

12	23	1	112	12	22	1	11222	1321
72	19	7	1224	80854	36463	57691	5981003	
R	O	Y	V	E	R	S	U	C
H	T	E	R	B	I	T	T	E
N	A	N	T	W	O	R	T	H
E	N	N	I					
S	O	M	O	S	A	X	X	S
O	M	O						
S	E	I	N					

This text is then taken out by columns according to the key and written horizontally in the second enciphering rectangle. In this rectangle the column whose number is the same as the day of encipherment and all squares on the top line to the left of the column having the number of the month are blocked out, and the text is started in the latter column. In our example the result would be:

12	23	1	112	12	22	1	11222	1321
72	19	7	1224	80854	36463	57691	5981003	
G	O	H	Y	A	G	I	Y	
E	U	B	R	E	U	I	I	
M	O	X	R	R	F	J	A	
D	I	R	V	G	Z	J		

The final step consisted of transcribing the columns in key number order from this rectangle and separating into five letter groups for transmission. Thus: - JHXR GGIJ JBLL, etc.

There was one exception to the foregoing procedure. This was that when the month and day were numerically equal the column designated by the day could not be blocked out in the second

TOP SECRET ULTRA

encipher diagram, because the text had to start in this column. In such a case the two transposition rectangles were both the same.

When all the cryptographic features of this system are analyzed, it is evident that here is a truly novel development. It is notable that, although a really complex cipher is produced, the system is based altogether on elements that can be easily memorized; that, although a given literal key phrase remained in effect for a long time, it would nevertheless produce a different pair of numerical keys for each day; and the combination of key lengths is such that the shortest message constituting a multiple of both key lengths would be 930 letters.

The use of variants for the most common letters in the language used was, of course, to suppress the outstanding frequencies of these letters and prevent or delay the identification of the language employed. By adding the element of complete substitution with variants to a difficult form of double transposition there was produced, cryptanalytically speaking, a really difficult system. Although the individual elements are simple and familiar processes, they were here combined and amplified into what appeared to be a truly formidable system and one for which solution, if possible at all, would require a large volume of traffic.

The use of variants for frequent letters (or camouflage) proved to be no great obstacle to solution of the substitution alphabet, and in some cases proved to be an aid to solution of the transposition. Furthermore, within the experience of this office, it never delayed greatly the determination of the language used. As will be seen in the explanation of the method of solution by key weights, it provided the only method of solution that even approached a general solution, (necessitating, however, the use of only messages which involved completely filled second encipher rectangles.)

The major weakness of the ABC Schlüssel was the fact that the complete solution of a message would enable the reading of all traffic enciphered with the same basic phrase. The effective period of a given key phrase varied from three to six months. Another fact useful to the cryptanalyst was that once the general details of the system were discovered, the key lengths of both transposition steps were always known. The fact that no column was blocked out in the second encipher diagram when the number

of the day and the month of encipherment was the same, afforded, for such days, a situation most favorable for application of the general solution. An example of such a case is treated in G 2 (3). In addition there were the more familiar approaches to the problem of double transposition, i.e., anagramming of two or more messages of the same length on the same day, use of "cribs" from messages read on other circuits or recipients, the omission of some of the steps of the process, etc. Therefore, daily and painstaking scrutiny of traffic on all Hamburg circuits was pursued, searching for evidence of any of the special cases mentioned above, as well as for messages of such lengths as required by the method of solution by key weights.

It should be mentioned that a change to a different key phrase was usually ordered by the control station in the final message sent in the current key, for example, "Use Key Number 2", "Use Key Number 3", or the like. In fact, it was this practice of signaling changes of keys or systems in the current cryptographic system which gave the first intimation of an "ABC Schlüssel" and supplied the information which resulted in the solution of traffic on one particular circuit. See G 2 (2).

2. SOLUTION: ABC SCHLUESSEL

a. RECONSTRUCTION OF THE SUBSTITUTION ALPHABET

The first step in the solution of the traffic of any circuit using the ABC Schlüssel was the reconstruction of the substitution alphabet. The method used to accomplish this was fairly uniform and hence will be described in general, as it would vary only slightly for any of the individual circuits solved.

As previously noted, the camouflage of frequent letters was not a serious impediment to identification of the language or recovery of the substitution alphabet. It was found that about 1,000 letters of cipher text was usually sufficient to accomplish these results. The following comparative frequency tables based on four different samples, two of plain text, without camouflage, and two with camouflage, show that except for the letters involved in the camouflage, the frequencies correspond well enough to identify the language and serve as a basis for matching cipher letters against the plain text letters.

TOP SECRET ULTRA

Plain Text		Camouflaged	Plain Text	Camouflaged
German		German	Spanish	Spanish
Clandestine		Clandestine	Clandestine	Clandestine
A	54	53	111	50
B	23	22	12	13
C	30	26	43	35
D	35	31	36	45
E	158	60	117	34
F	24	28	10	47
G	32	27	18	45
H	40	33	10	31
I	68	63	59	58
J	1	5	6	9
K	12	14	2	9
L	38	36	38	37
M	25	20	24	24
N	91	36	74	72
O	29	54	87	77
P	10	37	19	27
Q	1	23	8	11
R	71	73	80	71
S	56	56	72	67
T	57	46	42	42
U	49	48	40	42
V	10	16	12	13
W	17	21	1	34
X	53	91	66	79
Y	1	40	10	30
Z	15	41	3	4
1000		1000	1000	1000
				- Total

It is clear that we should be able to recover the substitution alphabet in most cases, by judiciously fitting the observed relative frequencies of the cipher text letters to the distribution of the relative frequencies obtained from previously deciphered plain text, adjusted for the camouflage element, and rearranged in the order required by the language involved for the plain component, keeping in mind the alphabetical considerations imposed by the key word method of deriving the cipher component. By relative frequencies we mean frequency count adjusted to the basis of 1,000.

For the purpose of clarifying the process of fitting a cipher component which had been derived by the keyed columnar method to

TOP SECRET UL

a plain component, consider the example from page 157.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8																		
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

It is clear that the different letters of the key word itself are distributed through the cipher component in alphabetical order and that the letters from each of the remaining lines of the key word transposition diagram are distributed through the cipher component according to the plain text order of the key word letters. Therefore, if the relative frequencies are matched so that a series of letters in alphabetical order is spaced at intervals which are uniform or vary by only one, and at the same time we get such uniformly spaced series which embrace practically all of the rarer letters, then by rearranging the order of the less frequent letters so that they progress alphabetically, the letters of the first line should form a plain text word without repetitions of letters. Most of the substitution alphabets were solved by this process.

To illustrate this method, let us follow through the actual solution of one of the substitution alphabets, one used by circuit U-41. After traffic had accumulated to the extent of approximately 1200 letters, frequency counts were made on all messages and totaled and the relative frequencies computed, with the following results:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Observed					1										1						1					
Frequency	1	2	3	6	5	4	3	5	1	8	3	3	0	1	5	0	1	9	1	5	4	2	2	7		
	6	3	6	2	0	9	3	5	6	8	7	8	2	9	2	6	4	2	7	5	0	3	2	3	8	6

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Relative					1																					
Frequency	1	1	2	5	4	4	0	4	1	7	3	2	8	4	8	1	7	4	3	1	2	6				
	3	9	9	0	1	0	8	5	5	5	1	1	6	8	9	5	3	3	4	7	8	3	4	9	3	2

Since U-41 was a Spanish circuit, the language used was assumed to be Spanish. The plain component was accordingly arranged for Spanish with the A between V and W, and with the previously computed relative frequencies for camouflaged Spanish

TOP SECRET ULTRA

Case (See page 100).

B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	3	4	3	4	3	5		3	2	7	7	2	1	7	6	4	4	1	5	3	7	3		
3	5	4	7	5	1	8	9	3	7	4	2	7	7	1	1	7	2	2	3	0	4	9	0	4

Now assumptions were made as to cipher equivalents of these camouflaged plain text values, based on the relative frequencies, and the considerations resulting from the manner of deriving the cipher component from a key word, as previously explained. Other facts which helped greatly were:

1. That the letter A almost invariably was one of the letters of the key word and so became the first letter of the cipher component and the equivalent for plain letter B,
2. That in Spanish Glandestone traffic the letter of lowest frequency was invariably K_p,
3. That the highest was Q_p or X_p.

After making the preliminary guesses, together with a tentative demarcation of the columns in the key word diagram, (a great deal of trial and error in placing the cipher letters is omitted from this description) the results were:

Plain	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	1	3	4	3	4	3	5		3	2	7	7	2	1	7	6	4	4	1	5	3	7	3		
	3	5	4	7	5	1	8	9	3	7	4	2	7	7	1	1	7	2	2	3	0	4	9	0	4
Cipher	A		G	D		I	Q	L		N	O		O		R		S						T		
	1		2	5				3		8	1				8				1				7		
	3		9		0		5	3	1	6	0		9		3				4				7		
											8														

This arrangement indicated a key word of 10 letters, with six 3-letter and four 2-letter columns. Now an attempt was made to place U, V, W, X, Y and Z, in conjunction with the letters already placed. Since these were rare letters, it was assumed that they were not used in the key word and therefore there would be no more than one of these letters in each column, and that they would always occur at the end of the long column.

TOP SECRET ULTRA

Plain	P	Q	R	S	T	U	V	W	X	Y	Z
	13434435	3277217	64415373								
	3856781093	74277117	222304904								
Cipher	A	B	C	D	E	F	G	H	I	J	K
	14324416	23811785414271									
	32495052536180931302453798										

The remaining letters were readily filled in, and after alphabetizing according to the U, V, W, etc. sequence we had

T A S E R D O L C I
B E F G H J K M P Q
U V W X Y Z

However, this arrangement did not produce a plausible key word. By changing the positions of Y, W and V in the cipher component, and discarding the assumption $G_p = D_p$ in favor of $G_p = F_p$, also $I_p = L_p$ in favor of $I_p = H_p$, we obtain the following complete cipher component :

Plain	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
	1	3	4	3	4	4	3	5			3	2	7	7	2	1	7	6	4	4	1	5	3	7	3	
	5	5	5	5	7	5	1	8	9	3	7	4	2	7	3	1	1	7	2	2	3	0	4	9	0	4
Cipher	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	1	4	3	2	4	4	1	6			2	3	8	1	1		7	8	5	4	1	4	2	7	1	
	3	2	4	9	5	0	5	2	5	3	6	1	8	0	9	3	1	3	0	2	4	5	3	7	9	8

This gives the following:

10 8 1 6 9 3 7 5 2 4
T R A N S F O R M C I
B D E G H J K L P Q
U V W X Y Z

The key word TRANSFORMATION is readily apparent. The illustration merely shows some of the steps and obviously incorrect attempts. With relative frequencies based on a more pertinent observation of previous plain language, together with a greater volume of cipher text frequency, greater precision might have been attained

TOP SECRET ULTRA

in matching the relative frequencies. However, each circuit showed individual frequency variations peculiar to itself, which introduced vagaries into the results of this procedure, whenever theoretical frequencies were used.

b. SOLUTION OF THE TRANSPOSITION KEY

The solution of the transposition key proved to be much more difficult than solving the substitution key. Most of such solutions were the result of special cases occasioned by careless cryptographic practices. Some of these breaches of security, surprisingly, were committed by the central stations.

Four examples of solution will be shown, each typifying a different special case and a short description of a more or less general solution. These are:

- (1) Solution of the transposition key by use of a complete crib. Circuit U-41, Hamburg-Spain.
- (2) Solution by means of a partial crib expanded by trial and error into the complete plain language message. Circuit 4-2, Hamburg-Vigo.
- (3) Solution by means of two messages where both transposition keys were the same: Circuit 4-X, Hamburg-Lisbon.
- (4) Solution from a recipher of a message from which one step was omitted. Circuit 4-P, Berlin-Madrid.
- (5) Solution by key weights.

c (1) SOLUTION BY MEANS OF A COMPLETE CRIB. CIRCUIT U-41, HAMBURG-SPAIN

In August of 1943, traffic appeared on a circuit later found to be between Hamburg and an unknown place in Spain. Traffic was spotty and of insignificant volume. For a period of time in 1944 only calls were heard and it was thought possible that the circuit was dead. However, messages began to appear again, but the total number throughout the life of this circuit amounted to only 86 messages. Statistical tests showed that the system employed was probably a combined substitution transposition method.

TOP SECRET ULTRA

Following the introduction of the "ABC Schlüssel" on the majority of the circuits in the Hamburg networks, and the information gained after the solution by the British of the special case on circuit 4-Q, it was presumed that circuit 4-41 was employing this specific substitution transposition method and tests were made in pursuance of this assumption.

The language was determined to be Spanish and the substitution alphabet was solved by the method described heretofore.

Exhaustive study and experimentation with the traffic at hand failed to reveal any cases which were susceptible of solution of the transposition key. Finally, on 13 April, 1945 the Hamburg control transmitted a message over all circuits which seemed to be simply different versions of the same plain text. This was confirmed when five versions of this message were read on circuits using known key words. These five versions varied only in accordance with the language used and the individual serial numbers contained in each message. The answer station of the U-41 circuit received a message of 255 letters, the same length as the version of this message transmitted to the 4-41 out station which was being read and was using Spanish as plain language. The sixth group of the U-41 messages had already been identified as the date indicator group and the key for the encipherment of the date had been worked out. The key was:

1 1 2 2 3 4 5 6 7 8 9 0 0 0
F R A N Z O E S I C H T N V

In the message mentioned above the sixth group was G H T F Z, which gave 13 as the date of encipherment (the first three letters of this group were always nulls).

The frequency distribution of the camouflaged plain language of the 4-41 version of the message sent to all out stations was compared with that of the cipher text of the U-41 message, thus:

TOP SECRET ULTRA

	h-AI	U-41
A	9	3
B	4	11
C	9	9
D	9	11
E	10	12
F	11	16
G	10	11
H	5	6
I	18	-
J	3	8
K	-	17
L	7	8
M	9	4
N	17	8
O	22	7
P	8	27
Q	7	9
R	20	3
S	26	16
T	11	9
U	10	9
V	3	3
W	3	2
X	16	3
Y	6	21
Z	2	22
	255	255

The new substitution alphabet for U-41 (which had been introduced shortly before) was recovered, by matching the U-41 cipher text frequency shown above with those of the camouflaged plain language frequencies of the h-AI version of the message, according to the method previously described thus:

Plain B C D E F G H I J K L M N O P Q R S T U V A W X Y Z
 1 1 1 1 1 2 2 2 1 1 1 1
 4 9 9 0 1 0 5 8 3 7 9 7 2 8 7 0 6 1 0 6 9 3 6 6 2

Cipher A T C Q E D V F M I L N K Z O J Y P B U R W S H X
 1 1 1 1 1 1 2 1 2 1 1 1
 3 9 9 9 2 1 3 6 4 8 8 7 2 7 8 1 7 1 9 3 1 2 6 6 3

TOP SECRET ULTRA

The key word used was PERSONIFICACION. The cipher text of the U-41 message was then converted by this alphabet to plain text except that the camouflage could not be removed from the frequent letters. This camouflage, however, did not constitute any hindrance in the solution of the transposition key.

The Spanish message of 255 letters which had been read on circuit h-41, as it appeared in the first enciphering rectangle is shown below in Figure 22:

	1	2	3	4	5	6	7	8	9	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	3	3
1																												
2																												
3																												
4																												
5																												
6																												
7																												
8																												
9																												

Now, according to our theory, this same message, with a different serial number at the beginning and possibly changed very slightly in other particulars, constituted the plain text of the message sent over the U-41 circuit.

The cipher text of this message as transmitted was:

NW NR 14 QR 52 BT

YPPZY	KDQS	SFSUN	QQZL	DUFFY
GHTFZ*	YKBJD	OSKTM	YOSSQ	PTTSJ
YISGJ	PSPTZ	ZSCQJ	KBHGY	SGEYP
LVLB	PKFEX	HESVE	ZCFTY	JEARD
				U
ZSCZN	UTZGF	YFZZN	POFPO	KHFFP
		D		
QMSAL	DHEGE	LXUSJ	ZQFJB	YJGPT
LDVUC	QYPZR	GLYJP	ELEBK	PDGNO

TOP SECRET ULTRA

IZPK	EPKL	JUDW	ZPKK	ARCN
ZPKK	PPBC	KYKP	PLPK	ZCCK
THPD	ZPPC	DECK	UPKP	NOCK
ZPTZ	PKKK			

2215 GMT

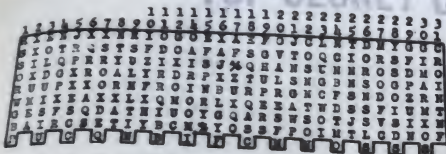
* Indicator group.

Now, we show this cipher text converted according to the substitution alphabet recovered:

RSSOR	NKPK	XIKU	KAKOL	DUIST
UNTQO	PKPK	PKPK	SOCKQ	NSKAK
SLSKO	OKSKQ	NTYAR	XATRS	ULHET
IKKPK	PKPK	OKSK	QKSK	OKSK
UOKAI	RICKO	IKPK	NSKX	AKKX
IKPK				
QKPK	OKSKQ	OKSKQ	OKSK	PKSK
ERSOV	AKRS	PKPK	SKAK	OSKX
TSOKL	QKPK	OKSK	PKPK	QKPK
SKPKD	OKSK	SLSK	OKPK	CKSK
OKSKS	QKPK	UKPK	MAKX	OSKRO

INTAF

This converted text was written in a 30 width rectangle omitting column 13, the column corresponding to the date of encipherment which was always blocked out of the second encipher rectangle in this system. The long and short columns were arbitrarily assumed to alternate through this diagram, as this arrangement would distribute the variation from the true division more or less evenly through all columns.



This diagram then had to be rearranged so that its rows would be made up, insofar as possible, of columns from Figure 22 written horizontally. When this was accomplished we would have the correct second encipher rectangle, and the order of the columns taken from Figure 23 would give us the key.

Column 16 from Figure 22 was chosen to be built from Figure 23 because of its low frequency letters. After trying several combinations, columns 25-15-67 from Figure 23 were put together.

Column 16 from
Figure 22 —

25 15 27
Y Y N
I F R
N S O
N P O
S N D
S R P
R E J Y V I G I
T C C

Here we had a trigraph J Y V from column 16 of Figure 22, (keeping in mind the fact that A, in the fourth line would be changed to Y). The other trigraphs in this arrangement were all found in Figure 22. They were extended from Figure 22 and columns in Figure 23 located to produce the necessary vertical combinations. Column ends from Figure 22 were marked as they were located.

TOP SECRET ULTRA

With the second encipher diagram thus reconstructed, it only remained to take out the horizontal text which had already been divided into column lengths, in the order of the key derived from the arrangement of the columns of Figure 23 (shown at the top of Figure 24) and write it into a 31 width first encipher rectangle vertically. The only column not placed by the key was No. 13, which had been omitted from Figure 23 and 24, and this was very easy to place so as to produce continuous plain text. The completely reconstructed first encipher rectangle of the U-41 message, with the camouflage not yet removed, is shown below.

1	1	1	3	2	2	2	1	2	2	2	1	2	3	1	2	2	1	1	1	1	7									
0	9	2	1	1	2	7	0	5	5	7	5	3	2	3	8	6	9	7	3	4	0	9	8	1	6	0	4	6	1	
L	F	Q	U	P	T	F	N	D	R	F	M	O	S	Q	U	F	I	N	T	F	R	R	U	M	P	I	R	T	F	M
P	O	R	X	L	M	G	N	T	T	S	G	R	V	I	C	I	O	D	G	J	X	N	D	O	L	G	P	O	R	L
U	P	R	O	N	T	O	S	I	N	C	O	N	T	Y	C	T	O	X	F	Y	V	O	R	S	H	Q	U	I	R	T
R	A	B	A	J	A	N	D	O	Y	E	S	P	E	R	A	R	N	U	E	V	A	L	L	A	M	A	D	A	X	S
I	Q	U	F	D	W	I	S	S	I	N	C	O	M	U	N	I	C	W	C	S	O	N	Q	U	P	D	F	N	U	S
T	G	D	G	S	S	U	S	M	O	N	S	X	J	S	S	X	C	I	G	E	O	S	A	Q	S	Z	A	Q	S	Z
X	E	O	R	Y	X	Q	R	X	X	Q	R	X	X	T	R	H	S	A	S	I	P	O	S	I	S	L	H	D	Y	H
E	M	O	S	C	O	N	F	I	R	M	A	C	I	O	N	K	Y	Z												

The actual starting point of the numerical key could be partially limited by placing on the correct line the letters involved in the camouflage. Thus it can be seen that the first letter at the top of column 19 must have been on the second line and the second letter of column 6 must also have been on the second line of the first encipher rectangle. Therefore, the end of the key must have been either number 6, 11, or 16. At this point, reconstruction of the literal key was the one final step necessary to complete the solution, and to provide the means for reading all the traffic on this circuit in this key. The literal key was soon recovered:

N	O	H	A	Y	P	E	C	R	L	U	C	H	A	Q	U	E	U	N	A	J	O	E	N	O	S	E	H	A	C	E
1	1	1	3	2	2	2	1	2	2	2	1	2	3	1	2	2	1	1	1	1	7									
0	9	2	1	1	2	7	0	5	5	7	5	3	2	3	8	6	9	7	3	4	0	9	8	1	6	0	4	6	1	

TOP SECRET ULTRA

0(2). SOLUTION BY MEANS OF A PARTIAL CRIB.
4-R HAMBURG-VIGO

This circuit had been first intercepted in April, 1943, and found to be employing a Janowski system of encipherment. All keys and text had been in German. On 5 July, 1943, there appeared the following message from Vigo:

"X AB MORGEN X SECHS X SIEBEN X
BEIINNEN MIT X ABC X SCHLUESSEL
UND NEUEN RUFZEICHEN ERBITTEN
BESTAETIGUNG"

Translated, the instruction reads:
"Effective morning July 6, begin with
ABC key and new call signs. Request
acknowledgement."

The first Hamburg message which could not be read by the old system, was a 60 letter message transmitted on the seventh of July, and enciphered on the sixth. This was assumed to be the acknowledgement requested by Vigo. The date indicator appeared in the 7th group and was the same as used in the previous system. The cipher text of this message was sent as follows:

NR 47 OR 13

FXKRN QXHPH OBWMI AUAGG VAMVS

GSJLV LMSDO*UGAGP FFYEG DHMQB

JWGVN AQSHB MSVMV

* date indicator group

Even with the practical certainty that here was at least a partial crib, no progress of any significance toward solution was achieved for a long time.

The solution of the substitution elements in use on this circuit was not a particularly difficult matter. Tests proved the language employed after the change in system was Spanish, not German. By matching expected plain text frequencies to cipher

TOP SECRET ULTRA

text frequencies in the manner described previously, an alphabet was derived based on the key word EXPECTACIONES. Thus:

3	10	7	2	9	1	4	6	5	8
E	X	P	C	T	A	I	O	N	S
B	D	F	G	H	J	K	L	M	Q
R	U	V	W	Y	Z				

It will be remembered that in Spanish A was moved from its normal position and placed between V and W in the enciphering alphabets. Combining the camouflage element with the monoalphabetic resulting from the above key word, four alphabets are developed to be used in successive lines of text. Thus:

Enciphering

Plains:	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
Cipher: I	A	J	Z	C	P	W	E	B	R	I	K	N	M	O	L	P	F	V	S	Q	T	H	Y	X	D	U
II							G	C	W	E													Y	H	X	D
III							K	O	C	E													X	Y	H	D
IV							E	J	W	C													D	Y	X	H

Returning to the message selected as the expected acknowledgement, it was studied in relation to the foregoing alphabets. In spite of the fact that the language used in the bulk of the messages appeared to be Spanish, it was decided from the frequency table of this message that it was in German.

It had been observed in previous Hamburg circuits that the internal serial numbers usually continued despite any change of system. In circuit 4-R the usual procedure was to place the internal serial number at the beginning of the message. It was possible, therefore, to make a strong assumption as to part of the plain text content of the message in question, i.e., that it started with either N K A Z W O A S I E B E N X or with Z W O S I E B E N X and that B E S P A E T I E N was the next word.

Below is a distribution of the cipher text of the message in question.

~~1~~~~2~~~~3~~ ~~4~~~~5~~~~6~~ ~~7~~~~8~~~~9~~ ~~10~~~~11~~~~12~~ ~~13~~~~14~~~~15~~ ~~16~~~~17~~~~18~~ ~~19~~~~20~~~~21~~ ~~22~~~~23~~~~24~~ ~~25~~~~26~~~~27~~ ~~28~~~~29~~~~30~~ ~~31~~~~32~~~~33~~ ~~34~~~~35~~~~36~~ ~~37~~~~38~~~~39~~ ~~40~~~~41~~~~42~~ ~~43~~~~44~~~~45~~ ~~46~~~~47~~~~48~~ ~~49~~~~50~~~~51~~ ~~52~~~~53~~~~54~~ ~~55~~~~56~~~~57~~ ~~58~~~~59~~~~60~~ ~~61~~~~62~~~~63~~ ~~64~~~~65~~~~66~~ ~~67~~~~68~~~~69~~ ~~70~~~~71~~~~72~~ ~~73~~~~74~~~~75~~ ~~76~~~~77~~~~78~~ ~~79~~~~80~~~~81~~ ~~82~~~~83~~~~84~~ ~~85~~~~86~~~~87~~ ~~88~~~~89~~~~90~~ ~~91~~~~92~~~~93~~ ~~94~~~~95~~~~96~~ ~~97~~~~98~~~~99~~ ~~100~~~~101~~~~102~~ ~~103~~~~104~~~~105~~ ~~106~~~~107~~~~108~~ ~~109~~~~110~~~~111~~ ~~112~~~~113~~~~114~~ ~~115~~~~116~~~~117~~ ~~118~~~~119~~~~120~~ ~~121~~~~122~~~~123~~ ~~124~~~~125~~~~126~~ ~~127~~~~128~~~~129~~ ~~130~~~~131~~~~132~~ ~~133~~~~134~~~~135~~ ~~136~~~~137~~~~138~~ ~~139~~~~140~~~~141~~ ~~142~~~~143~~~~144~~ ~~145~~~~146~~~~147~~ ~~148~~~~149~~~~150~~ ~~151~~~~152~~~~153~~ ~~154~~~~155~~~~156~~ ~~157~~~~158~~~~159~~ ~~160~~~~161~~~~162~~ ~~163~~~~164~~~~165~~ ~~166~~~~167~~~~168~~ ~~169~~~~170~~~~171~~ ~~172~~~~173~~~~174~~ ~~175~~~~176~~~~177~~ ~~178~~~~179~~~~180~~ ~~181~~~~182~~~~183~~ ~~184~~~~185~~~~186~~ ~~187~~~~188~~~~189~~ ~~190~~~~191~~~~192~~ ~~193~~~~194~~~~195~~ ~~196~~~~197~~~~198~~ ~~199~~~~200~~~~201~~ ~~202~~~~203~~~~204~~ ~~205~~~~206~~~~207~~ ~~208~~~~209~~~~210~~ ~~211~~~~212~~~~213~~ ~~214~~~~215~~~~216~~ ~~217~~~~218~~~~219~~ ~~220~~~~221~~~~222~~ ~~223~~~~224~~~~225~~ ~~226~~~~227~~~~228~~ ~~229~~~~230~~~~231~~ ~~232~~~~233~~~~234~~ ~~235~~~~236~~~~237~~ ~~238~~~~239~~~~240~~ ~~241~~~~242~~~~243~~ ~~244~~~~245~~~~246~~ ~~247~~~~248~~~~249~~ ~~250~~~~251~~~~252~~ ~~253~~~~254~~~~255~~ ~~256~~~~257~~~~258~~ ~~259~~~~260~~~~261~~ ~~262~~~~263~~~~264~~ ~~265~~~~266~~~~267~~ ~~268~~~~269~~~~270~~ ~~271~~~~272~~~~273~~ ~~274~~~~275~~~~276~~ ~~277~~~~278~~~~279~~ ~~280~~~~281~~~~282~~ ~~283~~~~284~~~~285~~ ~~286~~~~287~~~~288~~ ~~289~~~~290~~~~291~~ ~~292~~~~293~~~~294~~ ~~295~~~~296~~~~297~~ ~~298~~~~299~~~~300~~ ~~301~~~~302~~~~303~~ ~~304~~~~305~~~~306~~ ~~307~~~~308~~~~309~~ ~~310~~~~311~~~~312~~ ~~313~~~~314~~~~315~~ ~~316~~~~317~~~~318~~ ~~319~~~~320~~~~321~~ ~~322~~~~323~~~~324~~ ~~325~~~~326~~~~327~~ ~~328~~~~329~~~~330~~ ~~331~~~~332~~~~333~~ ~~334~~~~335~~~~336~~ ~~337~~~~338~~~~339~~ ~~340~~~~341~~~~342~~ ~~343~~~~344~~~~345~~ ~~346~~~~347~~~~348~~ ~~349~~~~350~~~~351~~ ~~352~~~~353~~~~354~~ ~~355~~~~356~~~~357~~ ~~358~~~~359~~~~360~~ ~~361~~~~362~~~~363~~ ~~364~~~~365~~~~366~~ ~~367~~~~368~~~~369~~ ~~370~~~~371~~~~372~~ ~~373~~~~374~~~~375~~ ~~376~~~~377~~~~378~~ ~~379~~~~380~~~~381~~ ~~382~~~~383~~~~384~~ ~~385~~~~386~~~~387~~ ~~388~~~~389~~~~390~~ ~~391~~~~392~~~~393~~ ~~394~~~~395~~~~396~~ ~~397~~~~398~~~~399~~ ~~400~~~~401~~~~402~~ ~~403~~~~404~~~~405~~ ~~406~~~~407~~~~408~~ ~~409~~~~410~~~~411~~ ~~412~~~~413~~~~414~~ ~~415~~~~416~~~~417~~ ~~418~~~~419~~~~420~~ ~~421~~~~422~~~~423~~ ~~424~~~~425~~~~426~~ ~~427~~~~428~~~~429~~ ~~430~~~~431~~~~432~~ ~~433~~~~434~~~~435~~ ~~436~~~~437~~~~438~~ ~~439~~~~440~~~~441~~ ~~442~~~~443~~~~444~~ ~~445~~~~446~~~~447~~ ~~448~~~~449~~~~450~~ ~~451~~~~452~~~~453~~ ~~454~~~~455~~~~456~~ ~~457~~~~458~~~~459~~ ~~460~~~~461~~~~462~~ ~~463~~~~464~~~~465~~ ~~466~~~~467~~~~468~~ ~~469~~~~470~~~~471~~ ~~472~~~~473~~~~474~~ ~~475~~~~476~~~~477~~ ~~478~~~~479~~~~480~~ ~~481~~~~482~~~~483~~ ~~484~~~~485~~~~486~~ ~~487~~~~488~~~~489~~ ~~490~~~~491~~~~492~~ ~~493~~~~494~~~~495~~ ~~496~~~~497~~~~498~~ ~~499~~~~500~~~~501~~ ~~502~~~~503~~~~504~~ ~~505~~~~506~~~~507~~ ~~508~~~~509~~~~510~~ ~~511~~~~512~~~~513~~ ~~514~~~~515~~~~516~~ ~~517~~~~518~~~~519~~ ~~520~~~~521~~~~522~~ ~~523~~~~524~~~~525~~ ~~526~~~~527~~~~528~~ ~~529~~~~530~~~~531~~ ~~532~~~~533~~~~534~~ ~~535~~~~536~~~~537~~ ~~538~~~~539~~~~540~~ ~~541~~~~542~~~~543~~ ~~544~~~~545~~~~546~~ ~~547~~~~548~~~~549~~ ~~550~~~~551~~~~552~~ ~~553~~~~554~~~~555~~ ~~556~~~~557~~~~558~~ ~~559~~~~560~~~~561~~ ~~562~~~~563~~~~564~~ ~~565~~~~566~~~~567~~ ~~568~~~~569~~~~570~~ ~~571~~~~572~~~~573~~ ~~574~~~~575~~~~576~~ ~~577~~~~578~~~~579~~ ~~580~~~~581~~~~582~~ ~~583~~~~584~~~~585~~ ~~586~~~~587~~~~588~~ ~~589~~~~590~~~~591~~ ~~592~~~~593~~~~594~~ ~~595~~~~596~~~~597~~ ~~598~~~~599~~~~600~~ ~~601~~~~602~~~~603~~ ~~604~~~~605~~~~606~~ ~~607~~~~608~~~~609~~ ~~610~~~~611~~~~612~~ ~~613~~~~614~~~~615~~ ~~616~~~~617~~~~618~~ ~~619~~~~620~~~~621~~ ~~622~~~~623~~~~624~~ ~~625~~~~626~~~~627~~ ~~628~~~~629~~~~630~~ ~~631~~~~632~~~~633~~ ~~634~~~~635~~~~636~~ ~~637~~~~638~~~~639~~ ~~640~~~~641~~~~642~~ ~~643~~~~644~~~~645~~ ~~646~~~~647~~~~648~~ ~~649~~~~650~~~~651~~ ~~652~~~~653~~~~654~~ ~~655~~~~656~~~~657~~ ~~658~~~~659~~~~660~~ ~~661~~~~662~~~~663~~ ~~664~~~~665~~~~666~~ ~~667~~~~668~~~~669~~ ~~670~~~~671~~~~672~~ ~~673~~~~674~~~~675~~ ~~676~~~~677~~~~678~~ ~~679~~~~680~~~~681~~ ~~682~~~~683~~~~684~~ ~~685~~~~686~~~~687~~ ~~688~~~~689~~~~690~~ ~~691~~~~692~~~~693~~ ~~694~~~~695~~~~696~~ ~~697~~~~698~~~~699~~ ~~700~~~~701~~~~702~~ ~~703~~~~704~~~~705~~ ~~706~~~~707~~~~708~~ ~~709~~~~710~~~~711~~ ~~712~~~~713~~~~714~~ ~~715~~~~716~~~~717~~ ~~718~~~~719~~~~720~~ ~~721~~~~722~~~~723~~ ~~724~~~~725~~~~726~~ ~~727~~~~728~~~~729~~ ~~730~~~~731~~~~732~~ ~~733~~~~734~~~~735~~ ~~736~~~~737~~~~738~~ ~~739~~~~740~~~~741~~ ~~742~~~~743~~~~744~~ ~~745~~~~746~~~~747~~ ~~748~~~~749~~~~750~~ ~~751~~~~752~~~~753~~ ~~754~~~~755~~~~756~~ ~~757~~~~758~~~~759~~ ~~760~~~~761~~~~762~~ ~~763~~~~764~~~~765~~ ~~766~~~~767~~~~768~~ ~~769~~~~770~~~~771~~ ~~772~~~~773~~~~774~~ ~~775~~~~776~~~~777~~ ~~778~~~~779~~~~780~~ ~~781~~~~782~~~~783~~ ~~784~~~~785~~~~786~~ ~~787~~~~788~~~~789~~ ~~790~~~~791~~~~792~~ ~~793~~~~794~~~~795~~ ~~796~~~~797~~~~798~~ ~~799~~~~800~~~~801~~ ~~802~~~~803~~~~804~~ ~~805~~~~806~~~~807~~ ~~808~~~~809~~~~810~~ ~~811~~~~812~~~~813~~ ~~814~~~~815~~~~816~~ ~~817~~~~818~~~~819~~ ~~820~~~~821~~~~822~~ ~~823~~~~824~~~~825~~ ~~826~~~~827~~~~828~~ ~~829~~~~830~~~~831~~ ~~832~~~~833~~~~834~~ ~~835~~~~836~~~~837~~ ~~838~~~~839~~~~840~~ ~~841~~~~842~~~~843~~ ~~844~~~~845~~~~846~~ ~~847~~~~848~~~~849~~ ~~850~~~~851~~~~852~~ ~~853~~~~854~~~~855~~ ~~856~~~~857~~~~858~~ ~~859~~~~860~~~~861~~ ~~862~~~~863~~~~864~~ ~~865~~~~866~~~~867~~ ~~868~~~~869~~~~870~~ ~~871~~~~872~~~~873~~ ~~874~~~~875~~~~876~~ ~~877~~~~878~~~~879~~ ~~880~~~~881~~~~882~~ ~~883~~~~884~~~~885~~ ~~886~~~~887~~~~888~~ ~~889~~~~890~~~~891~~ ~~892~~~~893~~~~894~~ ~~895~~~~896~~~~897~~ ~~898~~~~899~~~~900~~ ~~901~~~~902~~~~903~~ ~~904~~~~905~~~~906~~ ~~907~~~~908~~~~909~~ ~~910~~~~911~~~~912~~ ~~913~~~~914~~~~915~~ ~~916~~~~917~~~~918~~ ~~919~~~~920~~~~921~~ ~~922~~~~923~~~~924~~ ~~925~~~~926~~~~927~~ ~~928~~~~929~~~~930~~ ~~931~~~~932~~~~933~~ ~~934~~~~935~~~~936~~ ~~937~~~~938~~~~939~~ ~~940~~~~941~~~~942~~ ~~943~~~~944~~~~945~~ ~~946~~~~947~~~~948~~ ~~949~~~~950~~~~951~~ ~~952~~~~953~~~~954~~ ~~955~~~~956~~~~957~~ ~~958~~~~959~~~~960~~ ~~961~~~~962~~~~963~~ ~~964~~~~965~~~~966~~ ~~967~~~~968~~~~969~~ ~~970~~~~971~~~~972~~ ~~973~~~~974~~~~975~~ ~~976~~~~977~~~~978~~ ~~979~~~~980~~~~981~~ ~~982~~~~983~~~~984~~ ~~985~~~~986~~~~987~~ ~~988~~~~989~~~~990~~ ~~991~~~~992~~~~993~~ ~~994~~~~995~~~~996~~ ~~997~~~~998~~~~999~~ ~~1000~~~~1001~~~~1002~~ ~~1003~~~~1004~~~~1005~~ ~~1006~~~~1007~~~~1008~~ ~~1009~~~~1010~~~~1011~~ ~~1012~~~~1013~~~~1014~~ ~~1015~~~~1016~~~~1017~~ ~~1018~~~~1019~~~~1020~~ ~~1021~~~~1022~~~~1023~~ ~~1024~~~~1025~~~~1026~~ ~~1027~~~~1028~~~~1029~~ ~~1030~~~~1031~~~~1032~~ ~~1033~~~~1034~~~~1035~~ ~~1036~~~~1037~~~~1038~~ ~~1039~~~~1040~~~~1041~~ ~~1042~~~~1043~~~~1044~~ ~~1045~~~~1046~~~~1047~~ ~~1048~~~~1049~~~~1050~~ ~~1051~~~~1052~~~~1053~~ ~~1054~~~~1055~~~~1056~~ ~~1057~~~~1058~~~~1059~~ ~~1060~~~~1061~~~~1062~~ ~~1063~~~~1064~~~~1065~~ ~~1066~~~~1067~~~~1068~~ ~~1069~~~~1070~~~~1071~~ ~~1072~~~~1073~~~~1074~~ ~~1075~~~~1076~~~~1077~~ ~~1078~~~~1079~~~~1080~~ ~~1081~~~~1082~~~~1083~~ ~~1084~~~~1085~~~~1086~~ ~~1087~~~~1088~~~~1089~~ ~~1090~~~~1091~~~~1092~~ ~~1093~~~~1094~~~~1095~~ ~~1096~~~~1097~~~~1098~~ ~~1099~~~~1100~~~~1101~~ ~~1102~~~~1103~~~~1104~~ ~~1105~~~~1106~~~~1107~~ ~~1108~~~~1109~~~~1110~~ ~~1111~~~~1112~~~~1113~~ ~~1114~~~~1115~~~~1116~~ ~~1117~~~~1118~~~~1119~~ ~~1120~~~~1121~~~~1122~~ ~~1123~~~~1124~~~~1125~~ ~~1126~~~~1127~~~~1128~~ ~~1129~~~~1130~~~~1131~~ ~~1132~~~~1133~~~~1134~~ ~~1135~~~~1136~~~~1137~~ ~~1138~~~~1139~~~~1140~~ ~~1141~~~~1142~~~~1143~~ ~~1144~~~~1145~~~~1146~~ ~~1147~~~~1148~~~~1149~~ ~~1150~~~~1151~~~~1152~~ ~~1153~~~~1154~~~~1155~~ ~~1156~~~~1157~~~~1158~~ ~~1159~~~~1160~~~~1161~~ ~~1162~~~~1163~~~~1164~~ ~~1165~~~~1166~~~~1167~~ ~~1168~~~~1169~~~~1170~~ ~~1171~~~~1172~~~~1173~~ ~~1174~~~~1175~~~~1176~~ ~~1177~~~~1178~~~~1179~~ ~~1180~~~~1181~~~~1182~~ ~~1183~~~~1184~~~~1185~~ ~~1186~~~~1187~~~~1188~~ ~~1189~~~~1190~~~~1191~~ ~~1192~~~~1193~~~~1194~~ ~~1195~~~~1196~~~~1197~~ ~~1198~~~~1199~~~~1200~~ ~~1201~~~~1202~~~~1203~~ ~~1204~~~~1205~~~~1206~~ ~~1207~~~~1208~~~~1209~~ ~~1210~~~~1211~~~~1212~~ ~~1213~~~~1214~~~~1215~~ ~~1216~~~~1217~~~~1218~~ ~~1219~~~~1220~~~~1221~~ ~~1222~~~~1223~~~~1224~~ ~~1225~~~~1226~~~~1227~~ ~~1228~~~~1229~~~~1230~~ ~~1231~~~~1232~~~~1233~~ ~~1234~~~~1235~~~~1236~~ ~~1237~~~~1238~~~~1239~~ ~~1240~~~~1241~~~~1242~~ ~~1243~~~~1244~~~~1245~~ ~~1246~~~~1247~~~~1248~~ ~~1249~~~~1250~~~~1251~~ ~~1252~~~~1253~~~~1254~~ ~~1255~~~~1256~~~~1257~~ ~~1258~~~~1259~~~~1260~~ ~~1261~~~~1262~~~~1263~~ ~~1264~~~~1265~~~~1266~~ ~~1267~~~~1268~~~~1269~~ ~~1270~~~~1271~~~~1272~~ ~~1273~~~~1274~~~~1275~~ ~~1276~~~~12~~

TOP SECRET ULTRA

1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 3 3

(B) 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

A	M	A	F	O	M	M	U	V	V	S	S	L	H	A	F	F	E	D	H	B	H	O	A	R	B	S	M
B	O	H	H	B	W	A	A	G	A	V	G	A	V	G	G	F	Y	G	H	Q	J	V	W	Q	H	M	V

Thereafter the procedure was to anagram the cipher text in the B rectangle using any combination of the vertical columns in the A rectangle as the plain text.

It was only possible to accept or reject assumptions after putting 4 or 5 key numbers together, looking for confirmation as they were built up. If the reasoning was valid, all except possibly one vertical line of rectangle A could be found on the same horizontal line of rectangle B, although the letters would not necessarily be adjacent.

This gave a preliminary confirmation of the correctness of rectangle A.

Actual solution went forward in the following manner: OV, a column out of diagram A, could be formed only from column 7 and 12 of B, since there was only one O and V on the same horizontal line of B. Therefore 7-12 was an adjacent pair in the key.

```

  7 12
10 V |
  3 A

```

Since BA was not a vertical column in A, it must represent the bottom of one column and the top of another, unless of course A was a short column:

```

  7 12
10 V |
  3 A |

```

The only possibilities for the bottom of an A column were F and X. Therefore 7-12 must be followed by any column in B that had as its bottom letter F or X, i.e., 19, 23, or 27.

<pre> 12 1 10 V F af B A F </pre>	<pre> 7 12 23 es 10 V X mn 3 X . </pre>	<pre> 7 12 27 10 V A fl 3 A d </pre>
--	--	--

TOP SECRET ULTRA

The small letters represent the only possible column bottoms that could fit next to the three elements of key. By a process of trying all possibilities, the right case was eventually reached.

```

7 12 27 1
O V | A F |
| B | A Q | O |

```

As the building process continued, it became progressively easier because the columns left to select from were reduced in number. Ultimately the entire key and the key phrase were recovered.

```

FRANCOLLEGATRIUMFALMENTEAMALAGA
1 2 2 2 1 1 1 2 2 1 3 2 1 1 2 1 2 3 1 2 2 1
2 7 1 4 6 6 7 8 9 4 2 9 8 6 1 1 3 3 9 2 0 5 0 1 4 3 5 0 6 5 7

```

TOP SECRET ULTRA

- 0(3). SOLUTION OF CASE WHERE BOTH TRANSPOSITION KEYS ARE THE SAME.

4-X HAMBURG-LISBON

On 1 September, 1944, circuit 4-X put into effect a change in transposition key. Constant watch was instituted, while traffic accumulated, for a case for which solution might be possible. On December 12th the Lisbon station sent two messages, each of which was 250 letters in length. Not only did this provide a case of traffic in depth, but it also provided that special case wherein both transposition rectangles are the same width. The most interesting of all the factors in this particular solution, furthermore, was the use of camouflage letters to fix positions of columns.

It was stated earlier that the Germans hoped, by means of camouflage of high-frequency letters, to obstruct identification of the language used. It has already been demonstrated that camouflage did not delay the determination of the language--a particularly striking circumstance being that of circuit 4-R, which changed from German to Spanish simultaneously with the change from "Janowski" to ABC Schluessel (See solution). But moreover, in the circuit under discussion here, camouflage was an actual aid to solution.

The substitution alphabet for this period on circuit 4-X was based on the key word FORTBILDUNG.

Enciphering

Plaint: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher:	T	R	J	D	F	A	N	I	V	I	K	L	A	N	S	O	C	A	R	E	Y	T	H	Z	U	Q
	U														N	A	S	O						Z	H	U
															S	M	J	O						U	Z	H
	V														U	N	S	R								

The messages as sent were:

NR 22 GR 51

C88Z0 KJVD8 0TNP0 EXHMO EXEWO
 OEOXQ HECBZ BMQSY FKBUQ WDAHJ
 CQKZM YMCGB OSMIZ ZOHVM KOYDN
 NQQS0 EUPNK RMERT IKHEB OTENZ
 DOPNN OEMCS QCCCL ZZCQC QRFBU
 CZHRE GUFZ0 CCQFP ZNUCH ZQCUN
 MQZZY ZSQZO ZOSKZ UZUCB TMHCU
 ZSOBB RQHCH UAKSZ RZRQU DCHUN
 FGYSQ WDKZZ LLBNQ OQOUE WGTNN
 DNKZP GFEBQ QPKUE SEBJR BWMJW
 XHEZH

NR 23 GR 51

GRIBS QRZNC OFEEP CSKJH AISZH
 TGNBZ NZRQC QCKJH ZBPEH CVYGI
 BKOND SKCZG GSB0E ZTMBZ 9DZ3A
 GY0EB QQKHC R3JAQ GRPDX DD0ZE
 EECYH OECHE WQQFK QNBWY QZRMM
 QCRFZ HZZZB SHMZB AUCBA ZHZKH
 PQQZ B888E QQUCT IPRZF NNM7Z
 URZAN RSNEP SAKXH HZADQ PZZUG
 EEXCD FHPFM UZAAD NEESX EDEBZ
 FALKA Q4A40 UFZZE H44S4 N44RQ

TOP SECRET ULTRA

[illegible]

1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

1	I	O	P	E	T	X	O	P	A	U	I	S	E	I	S	T	P	A	Z	U	T	Y	U	X	I	D	A	E	U	R
2	T	R	L	W	Z	A	C	A	B	C	V	Z	F	E	G	R	Z	F	X	A	T	C	U	L	U	U	F	X	E	A
3	M	Z	B	I	R	D	P	Q	X	Z	G	C	Q	F	X	X	N	X	Z	F	X	P	C	U	N	U	U	F	X	E
4	A	F	E	O	Z	U	L	U	I	Z	Z	R	U	L	T	E	X	E	X	I	H	N	H	Z	S	Y	P	H	G	Z
5	F	U	G	A	R	E	R	X	G	L	I	X	R	Z	O	U	A	X	A	R	O	O	L	D	R	X	Y	M	I	P
6	Z	U	K	X	L	A	X	W	I	E	T	U	E	R	O	X	G	L	A	W	N	T	S	X	C	N	U	T	F	
7	T	D	P	O	B	L	I	N	N	R	D	U	A	A	Z	X	Y	E	A	K	F	P	E	X	F	G	C	L	X	
8	X	R	X	X	E	Q	I	A	Q	T	C	U	H	H	R	A	R	F	L	F	X	O	E	Y	E	C	U	Z	U	

After conversion of the cipher text into the letters resulting from the application of alphabet I, attempts were begun to solve the transposition key. Some effort was expended in attempts at anagramming, but due to the length the only tangible success was in isolating the probable beginning. As the external numbers were consecutive, from the pattern of message texts read previous to the change of key it was logical to expect "FTS X EINS" to begin the second message. The only suitable arrangement was:

C A R V A
F T S X E I N X

But no such cover name had appeared in previous traffic so this approach was not pursued further.

However, because of the fact that when the day has the same numerical value as the month no column is eliminated. in the second

enriching diagram, it was known that identical keys had been used for each of the transposition processes. Further, the length being 220, in each diagram there would be eight full rows of 22 letters each and two letters remaining, the position of one long column (12) being known (messages enciphered on the 12th day must begin under 12 of the key). If the column adjacent to 12 could be correctly chosen, therefore, the correct lengths of all columns in both transposition processes could be accurately determined. An assumption of column location in the key could thereby in many cases be confirmed or rejected on the basis of the resultant plain text positions of the more significant camouflage letters.

The two messages were set up for the general solution for double transposition* (see Figures 26 and 27) with all cipher text converted into the first alphabet.

Figure 26

1	2	3	4	5	6	7	8	9	0	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	3	3			
2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1		
3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5	5	8	8	8		
2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	
6	6	6	6	6	6	7	7	7	7	7	7	7	7	7	7	8	8	8	8	8	8	8	8	8	8	8	9	9	9		
3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	
9	9	9	9	9	9	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	4	4	5	5	5	5	
5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
5	5	5	5	6	6	6	6	6	6	6	6	6	6	6	7	7	7	7	7	7	7	7	7	7	7	7	8	8	8	8	
6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
8	8	8	9	9	9	9	9	9	9	9	9	9	9	9	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1
7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	

*For a full exposition of this method and terminology, see the Secret publication of the War Plans and Training Division, Signal Intelligence Section, entitled "General Solution of the Double Transposition Cipher." The following description is based on the assumption that the reader is familiar with this method.

Figure 28 Continued

Figure 26 Continued

2 4 9	2 5 0	2 2 0	2 2 1	2 2 2	2 2 3	2 2 4	2 2 5	2 2 6	2 2 7	2 2 8	2 2 9	2 3 0	2 3 1	2 3 2	2 3 3	2 3 4	2 3 5	2 3 6	2 3 7	2 3 8	2 3 9	2 4 0	2 4 1	2 4 2	2 4 3	2 4 4	2 4 5	2 4 6	2 4 7	2 4 8
-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------

Figure 27

[illegible]

Figure 27 Continued

Cipher
Plain

Cipher
Plain

C
C1
C2

Cipher	X	P	Z	Y	Q	X	Y	P	L	Y	Y	X	T	R	A	W	N	E	R	Y	X	P	I	A	A	T	Z	E	R	N
Plain	A	A	A	L	U	Z	Z	Y	R	W	K	F	T	X	F	H	O	N	F	X	Y	A	X	N	O	T	P	O	U	

185

TOP SECRET ULTRA

For the location of the column 12 number sequence there were two possibilities:

C ₀	89	90	91	92	93	94	95	96	97
C1	1	32	63	94	125	156	187	218	249
C2	U	A	Q	W	U	O	X	G	I
	C	S	G	G	R	X	U	U	U

or

C ₀	90	91	92	93	94	95	96	97	98
C1	1	32	63	84	125	156	187	219	249
C2	A	Q	W	U	O	X	G	I	D
	S	C	C	R	X	U	U	U	R

The significant Q in location 91 did not help here for it could have replaced either location 32 or 63 of C₀, both being possible fourth alphabet positions. All columns were then tried in the position following 12. For example, a test of column 2 (plain) in the 13th place (cipher) thus:

C ₀	98	99	100	101	102	103	104	105	106
C1	2	33	64	95	126	157	188	219	250
C2	D	O	O	Q	U	N	R	P	Z
	R	E	V	Q	U	R	E	A	H

This was an unqualified rejection, because the double Q was certainly a fourth alphabet substitution, whereas the above setup placed it in location 95 of C₀, which was a third alphabet substitution. Similar tests were made of all columns although of course in every case the result was by no means as definite as in the example given. The data thus obtained was compared with key weight scores for column 12, Column 8 appeared most favorable, so further experimentation was given to it first. It proved later to be the correct one; but had it not been, the same procedure would have been tried with each of the several other favorable columns.

The general solution setup with the assumption of the key 12-8 is shown in Figure 27. By the operation of the two columns thus located, the K/Q pair of column 8 was thrown to plain text position 219. Fortunately this was a unique pair, probably requiring a C/vowel pair to precede it in order to make good text (the "Q" being actually a fourth alphabet "N"). Since position 218 was already determined as replacing #97 by the action of column 12, and since #97 was in the fourth position of the column containing it (4-35-

66-71, etc.), it followed that the pair for position 218 must come from the fourth row of any one column. There were several C/vowel pairs but only one in the fourth position — the C/I in column 9. Testing this column for the h-35, etc. sequence showed excellent confirmation, since it operated to place the significant Q's in proper alphabets. If our work so far was correct, we had the key fragment 12-8-X-9. An attempt was then made to find a suitable column to follow 12-8. Of several possibilities, column 26 appeared most favorable, but at this point could not be confirmed.

On the 18th of December the Lisbon station transmitted three messages of length 260 and all in the same key. Again attempts were made at anagramming, but due to the rather great length only the first 8 letters yielded with certainty, as follows:

P I T T X R E F
 F T S X E I N S
 F T S X Z W O X

These were also set up for the general solution. Column 12 (the column designated by the month) of the second transposition sequence could possibly begin at any location from 89 to 119, but assuming the 20 long columns were evenly distributed, it probably began at location 96, 97 or 98. This portion of the work sheet appeared as follows:

Q,	94	95	96	97	98	99	100	101	102	103	104	105
C1	—	1	31	61	91	121	151	181	211	241	—	
C2												
	R	Y	L	S	O	S	Z	E	I	X	P	Q
	S	P	S	D	X	U	S	N	T	Y	M	C
	S	I	R	Z	S	P	S	H	T	G	S	D

The sequence 1-31-61-91, etc. (representing a column of the first encipher rectangle) was slid in the various possible positions. #1 under location 95 was immediately rejected, since it would imply a plain text Y. #1 under location 96 (as shown) was improbable, since that placed #181 over the I/T/T triplet which had previously been determined to occupy the second plain text position and therefore would have to come from the top of a column in the first transposition process; but #181 was a very poor location for the top of a column since it implied that 7 of the 9 columns numbered 23 through 31 would all be long columns and therefore adjacent in the key. Placing #1 under location 97 showed up well, since the #151 above the I/T/T triplet

TOP SECRET ULTRA

was an appropriate top of a column (which in this case would be column 19). A test under location 96 was poor for the same reason as under location 96. Similar tests were made for all probable locations and 97 chosen as the best.

With this setup it was immediately evident that the key fragment 13-19 must exist, since the second plain text letters (I/T/T) came from column 19 and the message began with column 18 in the first encipher diagram. Tests were therefore made on this key fragment in an attempt to locate it with reference to the 12-8-X-9 fragment, using the two 12 December messages and the procedure earlier described when locating column 8, and coupling this information with tests according to the key system. The arrangement 12-8-X-9-18-19 appeared most promising.

A second attempt was made to fit a probable column for the X position in the key. The assumed key fragment was set up in all other messages in the circuit which were perfect rectangles in the second encipher diagram, and the remaining columns tried in X position on the basis of the significant camouflage letters. Again column 26 was the best of several possibilities, although it was noted that it would not confirm the CAR/PTS message-beginning previously anagrammed. However, this beginning was discarded since to produce the only existing R/S pair as the third letters of plain text would require column 1, 2, 3, or 4 to separate 8 and 9 in the key, all of which had proved to be improbable in previous tests made. (Actually this beginning later proved correct as anagrammed, the rejection having come about because the R/S pair was incorrect, an R/Z pair being the correct one, with Z garbled for S.)

At this point an attempt was made to recover the literal key for the derived numerical fragment:

12	8	26	9	18	19
F	E	R	E	L	L
G	S	M	M		
N	T	N	N		

"GESELL" looked promising. "SCHAFT" was likely to follow it and end the key word. This would required column 27 to follow 19, which when tested yielded excellent combinations. Further progress was quite rapid, requiring only that a column of appropriate numerical value for the assumed literal key be chosen to adjoin the previous fragment, and since there remained only a few possibilities for each, the correct one was readily confirmed. This gave the numerical sequence:

TOP SECRET ULTRA

12 8 26 9 18 19 27 4 14 2 10 29
G E S E L L S C H A F T

The procedure from this point was quite simple. The two pairs of messages previously set up were utilized, as well as a pair of length 90 on 10 September (both columns 9 and 10 having been located in the key), and an assumption of additional column locations tested for suitability in all three sets of messages. The literal transposition key was thus found to be:

V E R S I C H E R U N G S A K T I E N
G E S E L L S C H A F T

TOP SECRET ULTIMA

9(b) SOLUTION BY RECEIVER OF MESSAGE IN WHICH ONE
STEP WAS OMITTED. 4-P BERLIN-MADRID

Early in 1944, after the knowledge gained up to that point concerning the ARC Schlüssel, a practice was adopted which was considered a convenience in reconstruction transposition keys. After sufficient text accumulated to enable the substitution key on a given circuit to be recovered, the cipher text of all messages was converted into first alphabet equivalents.

This permitted easy conversion of letters in handling anagram situations, etc., since all variable letters changed their identities according to the same pattern.

On one occasion there appeared in this first alphabet conversion a nearly complete plain text message. On 9 October, 1943, a message 33 groups, "Mr. 97", had been transmitted.

MR 97 OR 33

MYNAB DQCYS VNUVL BDSUV LBDSN
BDYMT*YDVNX QNVZP NYRUR ZELPT
UTDXU RTYNO WZURT KUNOW ZURTK
UNKZF OIPOY IRLLA PPARO JUYAE
QZPVD YOVJL BDYSV QSQNA RULBD
VSPSB TBXZM YSVLS PVLAZ HRZUQ
SUXAB MSUXA BMSTO

* date indicator group

The substitution alphabet used was:

TOP SECRET ULTRA

Enciphering

Plains: I A B C D F G H I J K L M N O P Q R S T U V W X Y Z
 II ON X
 III P H Y H
 IV Q H Z E
 Cipher: A P B C U E D V G H K I M Z K J Y L Q R P S B N T O

With the conversion to the first alphabet, this message appeared as follows:

1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
N	N	X	A	C	H	T	J	R	E	I	X	F	I	S	C	H	E	F	I	S	C	H	E	X	N
H	F	X	L	T	X	I	O	B	X	R	U	F	U	O	O	S	B	Y	F	Y	H	L	F	U	Y
R	X	Z	W	O	F	U	Y	P	F	X	Z	W	O	F	U	Y	P	F	X	P	O	V	Z	M	B
Z	R	M	U	S	S	A	B	B	A	U	Z	Q	F	R	A	O	T	O	B	I	H	R	Z	I	Q
S	C	H	R	E	I	T	E	T	X	A	U	F	S	C	H	I	E	B	E	C	Y	C	L	O	N
R	E	I	S	E	B	I	S	A	O	K	U	O	F	T	E	F	L	A	C	N	E	F	L	A	C
N	E	Y	Z																						

This appeared to be the circumstance which had been hoped for but hardly expected: namely, a message transmitted without the application of the transposition steps. The German habit of repeating proper names between X's indicates FISCHX FISCX, for the camouflage rules of this system require the substitution of X for E and E for X in the second line of a rectangle; XZWOFUENFXZWOFUENF appears with the required substitution of E for Y and N for P in a possible third line; the sixth line becomes entirely intelligible with O becoming N for ANKUNFTXFLACO; with Z becoming E and E, N in a possible 4th line, the complete crib is evolved.

TOP SECRET ULTIMA

formed by the variable or camouflage portions of the alphabets.
 In a German type alphabet this would be the cipher equivalent
 of the plain letters X Y Z and N O P Q.

We reproduce below a sample German alphabet:

2	3	8	4	6	5	9	10	1	7
B	E	R	G	K	I	S	T	A	L
C	D	F	H	J	N	O	P	Q	
U	V	W	X	Y	Z				

Plain:	I	A	B	C	D	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	II														O	N									X	E
	III														P	N									Y	E
	IV														Q	N									Z	E
Cipher:	A	P	B	C	U	E	D	V	G	H	X	I	M	Z	Y	J	Y	L	Q	R	F	W	S	N	T	O

If we trace through the enciphering process, it becomes obvious that in the first enciphering (31 width) diagram, certain vertical combinations of the variable letters are more probable than others. For example a T (Cipher) vertical digraph would be caused by an E

(Plain) occurring on the third and fourth lines respectively for the first diagram. On the other hand an O (Cipher) combination

would mean E (Plain), Z (Plain), or Z (Plain), any of which is much less likely than the E (Plain) above.

In completely filled second rectangles the above vertical digraphs are transferred horizontally into the second diagram and then scrambled by the operation of the second key. This method attempts to unscramble the columns on the basis of the variable letter digraphs formed between columns. A start is made in column 1, comparing it with each of the other 30 columns: column 1 and the column that adjoins it should produce more of the T O (Cipher) type digraphs than is expected by pure chance, whereas column 1 with any other column should merely produce pure chance digraphs. Thus, by this process the most probable column should be selected to follow column 1 in the adjacent position.

Log weights are made up based on the addition of the plain text frequencies of all possible plain text digraphs divided by the cipher text frequencies. Thus, the T O (Cipher) digraph would give the following plain text digraphs:

TOP SECRET ULTRA

(Cipher)
Alphabet I O

- 1 I Z
- 2 I Z
- 3 E Z
- 4 I E
- 1 I Z

I Z Plain frequency in German of I times the plain frequency of Z
 I Z Plain frequency in German of I times the plain frequency of Z
 E E Plain frequency in German of E times the plain frequency of E
 I Z Plain frequency in German of I times the plain frequency of Z

The total plain text probability for all is divided by the cipher frequency of T times the cipher frequency of O. The result is put into logarithms. There are 64 log weights for each of the 64 digraphs possible.

All completely filled second diagrams are considered simultaneously and each element of the key is compared with every other one. 31 x 30 comparisons in all are made.

It is also possible to consider columns one apart and two apart, and make weights for these. However, these values are more tenuous, and can only be used to corroborate the adjacent columns already selected.

This method was of value in attaining tentative placement of small segments of key and when used with anagramming or cribs it was helpful. Solution by this method alone was not achieved, principally because enough completely filled second rectangles were never obtained.

A very elaborate extension of this method was developed and used successfully by the British, to whom there was available far greater volumes of traffic. A complete description of their method may be studied in Volume II of the British "Encyclopedia of Clandestine Systems."

TOP SECRET ULTRA

3. PROCEDURE 62

a. INTRODUCTORY

At the same time that Oberinspektor Menzer instituted his extensive cryptographic reforms in the systems used by the Hamburg network, he also effected far-reaching changes in those employed by the Berlin center circuits. Combined substitution and transposition was introduced on these Berlin center circuits but not in the same form as used in the ABC Schlüssel. These systems were referred to by number by the Germans themselves, as Procedure 40, Procedure 62, etc. These procedures differed from ABC Schlüssel in the substitution process. In Procedure 40, a periodic substitution was applied to all letters of the message before the double transposition; Procedure 62* used only the camouflage of frequent letters.

b. CRYPTOGRAPHIC FEATURES OF PROCEDURE 62

Procedure 62 is a system based on double transposition with a camouflage of common letters.

The transposition key is derived from a key phrase of 31 letters in the following manner. The phrase is written out in two lines, the first line consisting of 16 letters with a vacant space after each letter, the rest of the phrase is written below under the vacant spaces left in the first line, beginning with the space that corresponds in number with the month during which the key is to be used, and returning to the beginning of the line to fill in the remaining letters. For example, in April the key phrase "LA MUJER MAS HERMOSA EN ESPANA DEL SUR" would be written thus:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
L	A	M	U	J	E	R	M	A	S	H	E	R	M	O	S
S	U	R	/A	E	N	E	S	P	A	N	A	D	E	L	

* The cryptographic system supplied to the espionage agents Colepaugh and Gimpel who were arrested on their arrival in the United States in December, 1944, appeared to be a Procedure 62 with the omission of the substitution process.

TOP SECRET ULTRA

The key phrase for this month would become:

L S A U M R U A J E E N R E N S A P S A H N E A R D M E O L S

The numerical key would be derived from this sequence in the usual manner.

The double transposition proceeds according to the following scheme; in the first enciphering rectangle the column directly before the number corresponding to the day of the month is struck out, making a numerical key of 30. All squares on the first line to the left of this column are also crossed out, and the message is written in, starting with the square under the number corresponding to the day of the month, and continuing on the following lines.

The camouflage of frequent letters is applied in this enciphering rectangle. In Spanish (the language used by the circuit discussed in the paragraphs on solution) the frequent letters A and E are camouflaged by the substitution of W, X, Y and F, G, H respectively in the following manner:

- Line 1 — plain
- Line 2 — A becomes W, E becomes F and vice versa
- Line 3 — A becomes X, E becomes G and vice versa
- Line 4 — A becomes Y, E becomes H and vice versa

This cycle is repeated throughout the message. The second encipher rectangle is used like the first except that no column is crossed out, making the key length 31. The text of the first rectangle is taken out by columns in the usual fashion and written into the second diagram horizontally, beginning with the square under the number corresponding to the day of the month. The final step consists of transcribing the columns from this rectangle in numerical order to form the cipher text.

c. SOLUTION

(1) SOLUTION BY MEANS OF A RECIPHER

4-AP was a circuit operated between Tangier in Morocco and Berlin. This circuit was quite distinct from 4-S, which has been previously described, although 4-S was also a circuit between Tangier and Berlin. So far as shown by the traffic of both circuits, there was no connection between the two.

TOP SECRET ULTRA

Violations of the basic rules of cryptographic security by careless or ignorant operators furnished the means of solution in this circuit. The first of these solutions was achieved when two messages which were obviously two cipher versions of the same plain text were sent, the first on 13 April, 1945 and the second the next day. There were a great many three or four letter repeats immediately apparent, and upon further study, it was concluded that the tops of the columns in the second cipher rectangle were correct, but that a mistake in encipherment had occurred which altered the placement of the lower parts of these columns. The last groups of the messages were altogether different and seemed to be indicators, consequently were ignored in the following steps. By placing both cipher versions in rectangles based on a 31 length key, and lining up the identical tops of the columns, (allowing for garbles here and there) a tentative division into long and short columns was obtained which was assumed to be correct.

CONCLUSION

1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 M P O O C K N C K O O S P M K R U W C W I Y S A O T E K
 D O Y N O K R N C K O O S P M K R U W C W I Y S A O T E K
 C O I K R R O L K S M I L K U I K R N K S K S M T T C L U S
 C M I S R D P S K S M L I S F C K O K H S R R G S D G O O L
 U T T R S K I K O R N T O V T I T K U O H R Y I K C G K N Y P
 R L E E L O U I S H T O U C C F 3 G O W O O F L

INCORRECT

D D O Y N O K R H G K O O S P E K R U N W C K X U Y S A O T E K
 F G I K R R O E L S M I L K A K R N K S S S E N T K C L U S
 N F R E D C K Z K S P O N I S D R S F N K I R L O I Q R R Q O N
 T N C N X T K U K R I T O C K K T T L T R O I T U N T K V K T
 L G O F Q F R Q L O I O U C U D E K S G W O N

The lower portions of the columns could now be matched. For instance, NTL, the lower part of column 1 in the incorrect message is identical with the lower part of column 2 in the correct message, PNC from column 2 is probably identical with VIC, the lower part of column 16 in the correct version, etc. By continuing this process the following series of identities was worked out (there were, of course, some ambiguities, but these could be eliminated by trial and error).

TOP SECRET ULTRA

(First line represents columns in the incorrect version — Second line represents columns in the correct version)

1. ~~1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 2 2 2 2 2 2 2 2 2 3 3~~
~~1 2 2 2 1 1 2 1 2 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1~~
 2. ~~2 6 5 7 8 7 8 1 9 4 7 3 9 6 8 6 3 5 0 2 0 3 5 1 9 1 2 4 4 0 1~~

Now by "chaining" these pairs, i.e., connecting vertical pairs by means of common numbers on the first and second row, the following sequence was obtained.

1 1 2 1 3 2 1 1 2 1 2 2 1 2 2 2 2 2 3 1 1 1
 1 2 6 6 7 3 5 9 0 0 2 3 9 4 6 1 0 4 7 2 3 5 8 4 1 1 7 8 5 8 (1)

This sequence, if the previous assumptions were correct, represented a cyclic (or decimated) permutation of the transposition key, with the decimation interval equal to the amount of displacement of the identical blocks at the ends of the two cipher versions.

The number of short columns in the incorrect message seemed to be one or two more than the number in the correct version. Consequently, the repeated blocks at the end were probably offset one or two places to the left in the incorrect version, so that the decimation interval to be applied to the recovered sequence would be one or two spaces. Upon trial it was found that the interval one (i.e., the sequence as recovered) would bring all the long and short columns together in both versions, and that the first long column was number 13, as shown below.

TOP SECRET ULTRA

1 21221 222 2231 11 1 11 21321
 1994610472358411785812667359002

K	C	N	L	S	E	K	G	O	E	I	C	K	T	P	K	K	N	X	M	C	T	P	I	R	E	F	M					
O	H	T	S	S	C	C	Y	A	W	X	N	O	U	K	K	K	R	P	R	D	D	K	O	K	O	Y	U	U	W	O		
I	L	L	L	T	S	X	X	X	X	S	R	C	S	S	S	O	R	K	E	F	G	U	R	K	I	M	N	O	K	M		
L	K	O	I	O	K	S	S	S	S	S	R	S	R	D	R	L	N	P	K	S	S	S	N	P	D	C	R	R	O	P	K	M
O	O	N	V	C	H	R	R	N	T	I	I	K	K	T	T	I	K	T	K	T	U	T	I	K	T	T	C	U	L	O	T	
T	I	C	C	O	S	S	E	O	G	O	E	F	N	K	H	O	F	U	U	R	L	C	C	C								

K	C	N	L	S	E	K	G	O	E	I	C	K	T	P	K	K	N	X	M	C	T	P	I	R	E	F	M					
O	H	T	S	S	C	C	Y	A	W	X	N	O	U	K	K	K	R	P	R	D	D	K	O	K	O	Y	U	U	W	O		
I	L	L	L	T	S	X	X	X	X	S	R	C	S	S	S	O	R	K	E	F	G	U	R	K	I	M	N	O	K	M		
H	K	O	I	O	K	S	S	S	S	S	R	S	R	D	R	L	N	P	K	S	S	S	N	P	D	C	R	R	O	P	K	M
O	K	V	C	H	R	R	N	T	I	I	K	K	T	T	I	K	T	K	T	U	T	I	K	T	T	C	U	L	O	T		
I	C	C	O	S	S	E	O	G	O	E	F	N	K	H	O	F	U	U	R	L	C	C	C									

Thus, having the key sequence, and the correct second enciphering rectangle, it was a simple matter to anagram the first enciphering rectangle according to the recovered key, and recover the original camouflaged text. The letters involved in the camouflage served to limit the actual starting point of the numerical key to two positions, and reconstruction of the literal key fixed the starting point absolutely.

E L C A B A L L E R O D O N Q U
 C H A / X J O T E D E L A M A N

1 11 1 1 213211 21221 222 223
 1785812667359002 199461047235841

N	C	I	O	N	K	K	U	N	O	K	T	R	N	
O	C	G	R	O	C	G	R	O	K	T	N	S	K	P
I	Y	K	K	U	N	O	K	H	M	P	I	R	H	K
L	A	S	E	K	L	E	I	T	L	K	D	O	S	
L	N	S	F	K	S	I	M	S	K	K	T	R	F	S
L	X	S	G	K	B	G	N	S	O	N	K	L	U	Z

T	R	E	S	U	N	O	K	C	O	N	T	I	N	U
S	P	O	R	T	F	K	N	U	P	V	F	C	P	R
I	R	G	C	I	D	O	X	L	K	C	I	C	I	L
K	D	O	S	K	C	Y	M	O	N	H	R	O	S	C
K	D	E	S	T	R	U	C	T	O	R	E	S	K	L
K	B	F	E	S	T	R	U	C	T	O	R	F	S	K

The recovery of the literal key was accomplished by writing out the numerical key in the staggered fashion used in Procedure 62 and then proceeding in the usual way, keeping in mind, however, that the plain text of the key must read alternate letters with each other, instead of adjacent letters. The key as recovered was:

11 18 8 2 6 3 19 20 13 29 26 10 27 23 28 31
7 15 1 16 17 25 30 12 9 14 21 4 22 5 24
E L C A B A L L E R O D O K Q U
C H A /I J O T E D E L A M A N

The last group turned out to be an indicator, as had been suspected. The letters were converted to numerals by means of the following table.

1	2	3	4	5	6	7	8	9	0
A	B	C	D	E	F	G	H	I	J
K	L	M	N	O	P	Q	R	S	T
U	V	W	X	Y	Z				

From these numerals were subtracted (non-carry-over) the numerical equivalents from the same table of the third group, the result being the enciphering date. In the message discussed, the last group KESZV becomes 15962 and the third group TLFOI becomes 02659, and subtracting as described above, the result is 13313, which should have been April 13, but was garbled.

It will be observed that here again the camouflage was found to be an aid to solution. In fact there is some basis for the assertion that this particular system would have had greater security with the substitution omitted entirely.

(2) SOLUTION BY MEANS OF A COMPLETE GRID

On the circuit just discussed, some messages were in a different key. In this class of messages the first group began and ended with Z (e.g. Z X V N Z), evidently to indicate that it used a different key or was directed to a different agent. The use of two keys in one system caused difficulty when the Z indicator was omitted by mistake or when key changes were made; hence the agents frequently sent questions and answers about the special key in the regular one.

TOP SECRET ULTRA

It was noticed that on 7 April, a 21-group message was sent with a 3 group not only at the beginning but at the end. On 8 April, the same message was repeated although the answer station had replied that it could not be read. Between these two messages a 20-group message was sent. Although the 21-group message had the 3 indicator, it was found to be enciphered in the regular key. Except for the camouflage and indicators, the two messages contained the same letters, hence were obviously two encipherments of the same letters, hence were obviously two encipherments of the same message. The camouflage aided here because it showed that the message extended into the fourth line, so that it was possible to determine within two squares the shape of the cage.

The deciphered message and the probable first deciphering diagram of the unsolved one (with the short columns distributed arbitrarily throughout the diagram) were compared and an anagramming procedure was used.

Solution on Regular Key

T	R	E	S	P	A	R	A	K	C	A	M	P	E	O	N	K	T	E	R	C	I	O	K	T	E	R	C	I	
O	K	S	W	L	I	O	L	I	W	R	S	F	I	S	K	V	I	W	K	S	F	V	I	L	L	W	K	I	E
E	G	T	U	X	N	K	O	L	C	X	N	O	K	U	N	O	S	G	I	S	D	O	S	N	U	G	V	O	R

Possible second Encipherment

1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
S	E	N	K	I	N	A	P	O	Y	N	I	K	O	X	F	I	D	R	I	C	U	V	E	K	Y	S	T	S	
K	L	G	N	O	K	I	O	L	T	A	I	X	A	M	F	K	I	X	S	C	U	N	L	K	O	P	I	L	K
S	V	C	E	R	K		S	K	Y	D	O	R	S	K		V	O	K	N	S	N	O		K	U	W	C	H	O

Since in enciphering, the columns of the first diagram became the "plain text" of the second, the columns of the unsolved version are matched to produce the columns from the deciphered version, horizontally. Taking CUG as a starting point, it is seen that there is only one Y in each diagram. It must therefore occupy the same plain text position, and must coincide as shown below. Thus, allowing for the camouflage, CUG becomes CUE, and TLN becomes TLE.

T	T	O	T
T	L	U	
C	Y	E	

Since the only possibility of completing the OU combination is to change the tentative placement of short columns, this is done and the anagramming continues until the entire diagram is filled in.

[illegible]

1 111212 115222212233 210 222
8969 312441456852009610327517837
X H O K N I V O C K Y P I K E S T T O T S W K I S P I N A
O K K L X A I L A S N M F O K L E T L U R K G N V O K W C O I
S I K K R D O G E S U E K I R K V C Y H T W G C F D R S S
CORRECT 1ST DECRYPTMENT

To derive the key, we find that column 1 of the correct decipherment is the same as column 8 of the correct division; column 2 is the same as 19, etc. The actual starting point of the key was determined by the camouflage, and the literal key "LA TELEFONICA ES UN EDIFICIO MUY ALTO", was derived.

L A T E L E F O N I C A E S U N
L A T O E D I F I C I O M U Y A

```

11 222 1 111212 11 2 212233 2
7817837896931244145655200961032
TRESKPARAKCAMPBONKTRCIC
KTFRCI
LLXKYK
NUHVHK
TOTSXNKGLCINOKUNOSGISDOS

```

The date indicator in this circuit proved to be the 3rd from the end, based on the 6th from the beginning.

TOP SECRET ULTRA

4. PROCEDURE 40

4. CRYPTOGRAPHIC FEATURES

This method of encipherment consists of:

- (1) Periodic substitution based on a 31 letter key phrase written in a square.
- (2) Double transposition based on the same key phrase.

The substitution step utilizes an alphabet square. The key phrase is written in a 5x5 square omitting repeated letters and the letter J, and followed by the remainder of the alphabet in normal sequence:

1

	D	O	N	E	M
	S	P	I	A	L
4	T	B	R	C	F
	G	H	K	Q	U
	V	W	X	Y	Z

2

3

The plain text is divided into groups of five letters to facilitate the substitution process, which is as follows:

(1) First letter of each group is replaced by the letter immediately above it in the square. Letters on the fifth line (VWXYZ) are considered as being above the first line (DONEM), e.g., P becomes O; N becomes X.

(2) Second letter of each group is replaced by the letter immediately to the right of it. Letters in the first column (DSTGV) are considered as being to the right of column five (MLFUZ), e.g., L becomes S; P becomes O.

(3) Third letter of each group is replaced by the letter immediately below it. The first line (DONEM) is considered as being below the fifth line (VWXYZ); e.g., X becomes N; R becomes K.

TOP SECRET ULTRA

(4) Fourth letter of each group is replaced by the letter immediately to the left of it. The fifth column (MLPUB) is considered as being to the left of the first column (DETOV), i.e., S becomes L; B becomes T.

(5) Fifth letter is plain.

(6) The letter J is plain in all positions.

The substituted text is then transposed twice with 2 different numerical keys derived from the same literal key. The numerical key is written across the top of an enciphering rectangle.

(1) First enciphering rectangle.

All squares on the top line to the left of the column whose number is the same as that of the day of encipherment are marked out. The substitution text is then written in the rectangle in horizontal lines.

(2) Second enciphering rectangle.

All squares on the top line to the left of the column having the same number as the month are marked out. The text is then taken out of the first rectangle in columns according to the key, and written horizontally from left to right into the second rectangle. To complete the encipherment the text is taken out of the second rectangle by columns according to the numerical key.

The cipher text resulting from the use of Verfahren 40 has two identifying characteristics:

(1) The letter, J, will have the same frequency as it has in the plain language being used.

(2) The frequency distribution for the remaining letters will not be as flat as a distribution of random letters since each letter represents its own plain text value one-fifth of the time.

b. SOLUTION: 4-AD MADRID-CEUTA

On 2 July, 1944 the Madrid and Ceuta stations began to transmit messages with characteristics that were unlike the machine enciphered messages sent from 30 March, 1944 through 30 June, 1944. The following factors were noted:

TOP SECRET ULTRA

(2) The letter, J, appeared in only a few messages, and its frequency in a single message was always low.

(3) No indicator was used. A date sometimes appeared in the preamble.

(b) The letter count was used in the preamble, whereas, the group count was used for the machine enciphered messages.

On 11 August, 1944 two messages with a letter count of 225 were sent from Madrid to Gerta, one at 1117 and the other at 1706. The two messages contained the same letters, and there were repeats seven and eight letters in length. It was evident that the plain texts were identical but that the keys for the last transposition had not been alike. The messages were written down and divided into sections of seven and eight letters according to the repeats, as shown below.

Mag. 1 PISRL PICLE FNTIC FRTG KICPE MACEN TNAE WISSE NQPU
30 16 17 18 7 26

Mag. 2 NPSIL PICLE PERIC MWOD HTAUR MOZNP ULURK NCEIC NQENS

7 8 9 10 11 12
LUED CLAPS CHIEP WITX NMEIM SPAUS LSUIC ILLJA QINOO
23 9 19 21 25 22
PAYCH IEPEN IGLTW LPSIE USAIT GSEHZ ANICE ACHAD IQKIS

13 14 15 16 17 18 19
CYOON MYSLM INSOE CYCEL QPERX EMACD DEATU PROZL IWLOS
6 12 13 31 4 15 10
BENNI GLP43 ILOOC YOORE WIFLN MIFBN ACN50 ECTNL NNDIM

20 21 22 23 24 25
TFLAS NNEKU DAETC SPOAH ADICE NSPAX GSEMK GYLIN ZANIE
8 24 29 20 27 14
KXOJ MFOCS ENRGY LICES MESIC ASIRM QASXM XPGIN MOOLN

26 27 28 29 30 31
MCEI ONLAS KOLPG IEFMC PIPEC EBETS NPSI LPARE WIFLN
5 28 11 1 2 3
MERTN ADEBP C.TP DAVEL SUICF ISULF MLEF NTYCF RWTG

TOP SECRET ULTRA

By chaining the above position numbers, the following key was obtained: 1-30-2-16-31-3-17-4-18-15-13-6-26-5-7-23-20-8-9-19-10-21-24-27-28-11-25-14-12-22-29. Since the long columns in the messages are 9, 10, 19, 21, 24, 27, 28, and 8 or 11, and since these numbers are adjacent in the key as derived, the above sequence was either the correct key sequence or the reverse of it.

In reconstructing the literal key the above sequence was examined. It was assumed that the key was in Spanish and that the numbers one through five represented the letter, A. It was assumed also that the last two words of the phrase were "LA" and a feminine noun ending in "A", and the starting point was adjusted accordingly. The literal key was found to be the proverb: DONDE MENOS SE PIENSA SALTA LA LIEBRA

2 2 1 1 2 2 2 2 1 2 1 1 2 2 3 1 3 1 1 1 1 2
7 3 0 8 9 9 0 1 4 7 8 1 5 4 2 2 9 1 0 2 6 1 3 7 4 8 5 3 6 6 5
D O N D E M E N O S S E P I E N S A S A L T A L A L I E B R A

The transposition key phrase was written in the substitution square, and the messages were deciphered. The mistake which had been made in enciphering the earlier message was the use of nine instead of eight in beginning the second transposition rectangle.

The same key phrase was in use when the transmissions stopped in February, 1945. However, the hand-system messages were sent only when the cipher machine was broken or new cipher instructions were delayed. Approximately one hundred messages were read.

PART II. DEVICES AND MACHINES

A. SCHLUESSELRAD

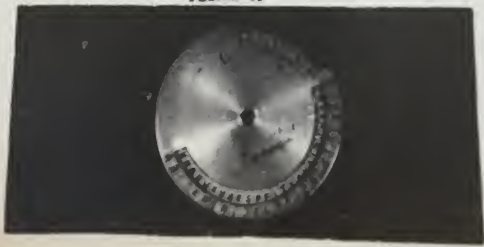
1. DEVICE USED IN CHILE

The Schlüsselrad was a hand-operated cipher device comprising two disks, one showing on its periphery the digits 0 to 9, plus the standard alphabet A to Z; the other showing on its periphery a key-word mixed alphabet. The latter disk was provided with teeth or notches, into which could be inserted a stylus or pencil for revolving the disk in process of encipherment. Figure 28 shows the two disks separately, and Figure 29 shows them together ready for use. (Photographs from a device captured in 1944.) A curious fact was observed: note that the inner disk sequence, the cipher component, has the same sequence as the plain component for the Kryha machine (see Part II, B).

FIGURE 28



FIGURE 29



TOP SECRET ULTRA

Different disks with different mixed alphabets were provided. The purpose of the numbers was to facilitate the use of an external key for encipherment which produced a polyalphabetic cipher with a fairly long period. A keyword of eleven letters was chosen and numbered alphabetically in the usual manner, dropping the first digit of two-digit numbers. Thus:

A	N	T	O	F	O	G	A	S	T	A
1	6	(1)0	7	4	8	5	2	9	(1)1	3

This numerical key was extended by adding two figures for the number of groups in the message and following with 4 numbers for a time-group. The first of the two foregoing requirements in the prescribed system thus prevented any message of more than 99 groups being sent; the second was for the purpose of preventing any two messages having exactly the same numerical key, since the time-group, which might be the true time-group or otherwise, would always vary.

A N T O F O G A S T A
1 6 9 7 4 8 5 2 9 1 3 1 5 1 4 4 9

The number of groups in the message and the time-group chosen were transmitted with the message, in plain text in the preamble. A fixed starting point was set for the two disks at the beginning of the encipherment; for example U must be in juxtaposition with U. The lower disk was moved in clockwise fashion, by inserting a stylus or pencil in the notched section of the disk, each notch in turn being designated by the key number above the particular letter to be enciphered. (All the foregoing requirements combined to produce a self-generating key, or autoclave.) With the numerical key from the key word previously shown, plus the number of groups in the message, plus a time-group, the following message would be enciphered thus: Setting the two disks in position U to U for the starting point and inserting pencil or stylus in the notch adjacent to the figure 1, the disk is revolved clockwise until stopped by the edge of the upper disk, the letter F in the normal alphabet is noted and the letter opposite it on the lower disk is recorded as the cipher letter; the lower disk is then moved again by inserting stylus in notch opposite the number 6 and the cipher letter opposite U is recorded; and so throughout the message.

TOP SECRET ULTT

Keys
Plain text:
Cipher text:

1607485291312144016074852
ZUERWILLLEHAIIEHALLBWOHLX
OPCVBAJHUYKFVQOKHAKVJHRA D

9131214401607416074852913
WIEGERTSMITINHMXORUESSSEX
HVTNHCPTZWHHPNKLZAZRZHIHEW

121440160
ALBERTOIX
EHIDFIRBB

TOP SECRET ULTRA

A. SCHLUSSSELRAD

2. DEVICE USED BY JOULE WITH ARGENTINE STATION

The JOULE cipher device was an autoclave and was used by the German agent LUNA in Argentina to communicate with "JOULE" at sea. "JOULE" was a sailing vessel which crossed the Atlantic with a cargo of supplies, radio equipment, and Enigma machines for the agents in Argentina. This special-purpose device operated mechanically exactly as did the Schlüsselrad found in Chile. However, both disks in this case carried mixed alphabets, based on key-phrases.

The instructions for using the "CHI RAD" system, as it was called at this time by the Germans, transmitted from Berlin to Argentina on 7 June, 1944, were as follows:

1. Message heading to consist of time and group count.
2. Upper slide of device to equal plain alphabet.
Letters: F E S T O M A U R I N D H O L B C K P Q V
H A Y Z written from left to right.
3. Lower slide to equal cipher alphabet. Letters:
H E U T M S D I O L O C K W R N F Z A B P Q V A Y
written in twice from left to right.
4. Letter J to be omitted and replaced by I.
5. The numerical key to be derived as follows:
Multiply the time by secret number 135, then progressively add the product. Example: Time 1610 x 135 equals 217350. The numerical key would be 217350 381085 11191613 etc., until 125 numbers were written out, after which the derived numerical sequence would be written in reverse. The numerical sequence of 250 digits to be repeated as often as required by message length.
6. Starting point plain L opposite cipher F.
7. Punctuation: Y equals period. X equals brackets.

TOP SECRET U.S.

However, Argentina did not understand how to derive the numerical sequence as shown in the example above, and on 20 June sent the following message in plain text to JOLLE. "Number system not clear. Please use only the following numbers: 327861649782331."

About ten messages were sent using this numerical sequence. On 25 June, Argentina, evidently fearful for security, requested that after 25 June the numerical key 327861649782331 be multiplied by the secret number 135 so that 17 digits would result.

Since the German control station was so obliging as to forward instructions in a system being consistently read, and the Argentine station was so naive as to send inquiries and instructions in plain language, no cryptanalysis was necessary to read all messages transmitted for this special purpose.

TOP SECRET ULTIMA

PART II, B. KRYHA

1. HISTORY

In message 548 from Argentina to Berlin on 20 January, 1943 Kryha Liliput was mentioned. This message was in a double transposition system which was being read by Coast Guard. A transposition of the message read as follows: "INTER. Your radio telegrams after number 395 no longer decipherable. How do you encipher? Have you key wheels with 26 fields on hand there? We should like to start with key wheels as soon as possible. Sequence of letters as in "Bolivar" under Kryha Liliput. Please reply soon." On 28 February, 1943 message 584 was sent from Argentina to Berlin. "LEIT. Following messages all enciphered with numbers. Starting position number 1 and A opposite A. Test message begins with last name of "SC". Hello boy, now we are off. Close all even numbers. Outer scale according BOLIVAR."

2. SOLUTION

With the active holes and starting position of the control wheel known, the corresponding holes were opened on a similar machine on hand at the Coast Guard Unit; the letters were arranged in the order of the normal alphabet on both the fixed and rotating sequences. The machine was set with the plunger in hole number 1 and the sequences aligned with "A" on the rotating sequence opposite "A" on the fixed sequence. This position of the sequences was called the "A" alphabet; the lever was pressed and when the rotating sequence stopped the letter opposite "A" on the fixed sequence was noted and recorded as the identity of the alphabet used for the encipherment of the second letter, etc. This procedure was continued through the full cycle of 676 as follows:

HOUBJ PVDJ QXDK RZFM SZON VBI OX
 KLR YQMS AGNUAH ONWC J PWDK SYFLU
 BIOVD J P XDK R XELT ZGMTAHPVCIR
 YFLSAGNUAH OUBIQW DJQX EMSZFO
 VCIPXDJRXELRYFNTAGNUBJPWCL
 SZFMUAG OUBIOVCKQXDKRYQMTZI
 PWCJRXIDLRYFLSZHNUAH OVDJQWY

TOP SECRET M/T

HTZGOUAIOVCIPWEKRKELSA GNTC
 JQWDLRIFLSZFMTHOURIPXAKQE
 GNTAIOUCIPWCJQYELRYFMUHXNW
 DKQXFLRZFMTHGWEVHIOVCJRUEKT
 AHNUCICOWCJQWDKSYFLSZGOREBHQ
 XEKRZFLTZGNTAHPVCIPWDLOYEN
 UBHOWCIQWDKQXIEMSZFMTAILVBK, etc.

IBM tabulating cards were then prepared, numbered from 1 to 676, each containing the arbitrary identifying letter of the alphabet used for the encipherment at cipher text position corresponding to the number on the card.

Between 28 February, 1943 and 12 March, 1943, 8 messages, numbers 586, 587, 589, 590, 611, 616, 617 and 618, containing a total of 2,300 letters were transmitted from South America.

These messages were punched on IBM cards, 1 letter per card, and the alphabet sequence on the previously prepared master cards was then reproduced on each message. Following this, the cards were all sorted together, first on the key letter and second on the cipher letter. The cards were then tabulated and a count made on the occurrences of each cipher letter through the 26 alphabets. The result of this tabulation indicated random distribution.

It was then conjectured that the first letter of each message was not enciphered at the starting position given, but that the lever was pressed once before the encipherment of the first letter. This theory was tested by removing one card from the top of the pack of key-sequence cards and reproducing the new key-sequence on all messages. The cards were then sorted and tabulated as before, with the result shown in Figure 30. In this figure the key alphabet is shown at the side of the figure and the cipher letter at the top.

TOP SECRET ULTRA

FIGURE 30

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	8	4	5	3	0	4	2	2	3	1	2	1	8	3	2	3	2	8	1	1	1	4	4	2	0	2
B	2	3	1	2	3	1	1	2	3	1	7	0	0	1	1	1	2	6	4	3	6	1	2	1	5	2
C	0	5	6	6	8	2	7	3	3	5	7	1	7	5	5	3	6	2	2	1	1	1	0	2	5	0
D	1	2	3	0	1	0	7	1	6	2	1	1	2	1	0	1	1	2	5	6	0	7	7	9	3	5
E	2	2	3	2	3	3	0	5	0	3	1	4	3	0	1	1	2	1	3	0	1	9	4	8	0	1
F	5	1	9	1	7	3	1	3	0	6	2	1	1	3	7	7	1	1	2	8	4	1	0	9	0	1
G	5	2	1	9	2	5	9	2	0	5	3	4	3	1	5	4	2	1	0	5	1	2	8	3	0	2
H	7	2	5	1	3	1	4	2	0	1	1	2	9	0	1	1	0	3	3	1	0	4	6	4	3	4
I	4	4	2	1	2	2	4	2	9	3	8	4	1	0	4	5	6	1	1	2	3	0	1	2	0	3
J	3	7	1	2	5	8	0	0	1	5	1	2	8	1	4	0	3	3	1	1	2	3	4	1	1	1
K	1	3	6	1	1	5	0	0	2	2	3	2	1	8	6	1	5	2	1	7	5	1	4	4	7	2
L	1	1	1	1	3	1	4	2	3	0	1	0	1	4	7	2	1	7	0	2	0	6	1	4	2	6
M	5	3	3	1	2	3	4	0	4	2	3	1	1	3	2	2	2	0	6	1	3	2	2	4	4	1
N	2	7	1	1	3	3	2	3	6	2	3	2	0	0	0	1	1	9	1	2	2	6	1	1	4	6
O	7	7	5	3	1	1	8	5	2	1	0	4	6	4	6	5	1	0	2	5	4	8	2	2	7	1
P	0	1	2	0	5	0	2	3	3	2	7	2	1	5	7	6	3	1	1	1	2	8	2	5	0	2
Q	2	2	4	1	1	1	0	7	5	1	6	3	6	0	2	9	0	4	5	2	5	6	0	2	3	2
R	1	6	0	2	4	2	4	3	5	6	3	1	0	6	1	4	4	4	2	5	4	1	3	1	4	7
S	2	0	0	1	4	4	0	5	1	2	3	2	5	6	2	4	0	0	2	2	0	0	9	4	7	1
T	1	2	6	1	3	6	3	1	3	5	2	3	2	7	4	6	0	7	2	5	1	1	3	1	5	2
U	1	3	6	4	2	3	3	3	2	1	2	6	0	8	1	6	8	8	6	5	5	5	2	9	2	4
V	6	2	2	1	3	0	1	4	1	2	4	2	1	2	3	1	3	6	8	5	0	2	2	0	7	2
W	6	3	3	4	8	1	1	0	6	5	1	0	2	3	1	1	2	3	1	5	3	5	1	2	0	2
X	1	0	3	1	4	8	1	0	1	4	2	3	2	0	1	3	1	0	4	4	8	1	2	6	1	5
Y	3	2	5	5	2	0	8	5	2	0	1	6	2	2	4	2	9	0	0	7	3	1	0	2	1	1
Z	8	0	2	3	3	2	1	0	4	7	0	1	2	5	5	2	3	8	0	2	5	3	1	6	5	1
A	8	4	5	3	0	4	2	2	3	1	2	1	8	3	2	3	2	8	1	1	1	4	4	2	0	2

1 1 1 1
 98998786889098988809908079
 96178882748239659906462506

2350

The vertical distributions were then matched with a slide or offset of 1 position to find adjacent letters in the cipher component. With distributions of the size shown in Figure 30, most of the distributions could be matched at sight without calculating the sum of the cross products of the individual frequencies for each juxtaposition.

TOP SECRET ULTRA

This procedure recovered the following cipher component:

S V G D W M Q C J A H T E X R P N F I K U B Z L Y O

This sequence was then substituted in the machine for the normal alphabet sequence on the rotating disc, the plunger placed in the correct starting hole and a short portion of cipher text converted to a monoalphabet, in terms of the standard alphabet on the fixed sequence, by advancing the machine through successive positions.

This monoalphabet was then solved to recover the following plain component which was then substituted for the standard alphabet on the fixed sequence:

E S P F I T V O N A L D C H R B G J K M Q U W I X Z

3. LATER DEVELOPMENTS

Shortly after the solution of the Kryha machine as used by Circuit J-W, the current traffic (in a different system) disclosed that, in an attempt to add additional security to Kryha messages, the German station would begin to transmit blind, using the call JLA, over the German Naval transmitter, and would simulate Naval traffic in all external appearances, with the exception of the serial numbers. The Argentine station continued to send this type traffic in 5-letter groups.

As the Kryha traffic progressed, the wear and tear on the LILIPUT model began to show its effect. It became necessary, on short notice, to close additional holes in the control wheel.

Finally, as the Kryha became more and more unserviceable, a new Enigma called the RED machine, was issued to the Argentine end of the circuit, and the Kryha messages disappeared from the traffic.

TOP SECRET ULTRA

PART II, C. ENIGMA: WHEEL WIRING UNKNOWN.

1. SINGLE TURNOVER. MAN-RDA-NDR

In January 1940, Coast Guard monitors intercepted suspicious traffic using the calls MAN V NDR, RDA V MAN, and the like, transmitting one to five messages daily. It shortly became apparent that whatever the system, all messages were enciphered from the same starting point. Aligning the messages showed frequent repetitions, particularly striking in 2, 3, 4 and 5-letter repeats at the beginnings, and occasional, even longer, repeats in the body of the messages.

Attempts to solve the first twenty or thirty messages in depth met with no success because of badly garbled copy and lack of any definite evidence as to language. However, by the time some sixty or seventy messages had accumulated, it seemed certain that the language was German and that a word separator had been used. The messages were then solved in depth out to a point where the depth had decreased to about half of its original amount. As solution progressed, incoming traffic increased the total depth to 110 messages.

In the progressive development of the plain-cipher equivalences for each position of the superimposed messages, it was observed that no plain letter was represented by itself in the cipher text and that the plain-cipher equivalences within each alphabet were reciprocal. These facts were of considerable help in extending the solution in depth, as was also the use of the letter X as a word separator. However, as the depth decreased, because of very unreliable copy in many places, the extension of the plain text became more and more difficult.

By this time there seemed ample justification for assuming that this traffic had been enciphered on an Enigma Cipher Machine. There was available to this office a model of the commercial version of this machine, together with the original manufacturer's instructions and suggestions for its use. These suggestions included the practice of using X as a word separator, and of representing numbers by their equivalent letters as shown on the keyboard of the Enigma machine:

1 2 3 4 5 6 7 8 9 0
Q W E R T Z U I O P

TOP SECRET

These procedures were followed in the traffic, together with other suggestions for bracketing enciphered numbers between Y's and using other combinations of X and Y for punctuation. However, the strongest evidence supporting this assumption was in the nature of the recovered alphabets. At this point, all the reciprocal alphabets recovered (approximately 75 had been practically completely recovered) were apparently independent of each other, and of any systematic or symmetric generic process. In other words, the cipher alphabets apparently were not generated by any conventional use of a Vigenere square, which rendered unlikely the use of any hand system. The Enigma machine was, therefore, the most likely known device which would never encipher a letter-as itself, and which would produce a long non-repeating series of apparently unrelated reciprocal alphabets.

The mechanical operation and variable elements of the Enigma machine were studied. It was observed that the wiring from the keyboard and the lightboard, to the end plate facing the exterior contacts of the outside wheel, was a constant element of the machine; and this created a belief that, if the effect of this constant element were eliminated from both letters of the plain-cipher pairs, a table of the resultant circuits through only the four wheels (and back to the outside of the first one) might provide a basis for predicting additional wheel circuits, from which additional cipher alphabets might be derived. (Note: At this point, there had been conceived a vague idea that as in the solution of the Hebern machine, there might be constructed a basic sequence which would be a function of the outside wheel and which could be manipulated to produce the successive cipher alphabets. What was being groped for, was of course a RCD square; but at the time such a table was unknown.)

Figure 31 shows alphabets 1 to 32 insofar as they were recovered from reading the messages in depth. Also included are alphabets 58 and 84 as they were completely reconstructed later. The plain-cipher equivalences are written in the order necessitated by considering the keyboard sequence order as the plain component. This seemed logical since this was the sequence of letters wired to the end-plate facing the exterior contacts of the outside wheel--reading the sequence in the direction in which the normal alphabet progressed on the rings of the wheels. The first 32 cipher alphabets are formed, therefore, by pairing the "QWERTZU" sequence with each line of the table in succession.

TOP SECRET ULTRA

FIGURE 31

QWERTZUIOASDFGHJKPYICVBNML

1	D	V	F	B	Y	K	N	M	C	J	G	Q	E	S	U	A	Z	X	T	P	O	W	R	L	I	N					
2	I	V	O	U	T	Q	R	N	L	P	Y	J	B	G	U	N	C	D	G	K	E	F	H	J	A	S					
3		C	Z	E	R	N	S	L	X	I	M	V	J	B	G		T	A	N	T	J	Z	X	I	F						
4	K	G	T	E	C	B	H	M	D	P	I	O	L	W	U	V	Q	A	S	V	E	R	Y	W	H	D	J				
5	P	B	X	C	I	S	O	T	U	F	Z	M	A	K	N	E	T	W	G	T	I	U	M	W	B	H					
6	L	K	H	O	J	N	F	B	R	G	M	Y	U	A	E	P	L	S	U	B	O	A	D	V	B	X	P	X	T	S	Q
7	N	F	A	Y	C	X	D	R	J	O	E	P	L	S	U	B	O	A	D	V	B	X	P	X	T	S	Q				
8	E	I	Q	V	M	P	J	W	P	Y	H	N	Z	X	S	O	Z	W	A	D	V	B	X	P	X	T	S	Q			
9	N	K	G	I	S	J	L	R	H	P	T	Y	M	E	O	Z	W	A	D	V	B	X	P	X	T	S	Q				
10	R	G	Z	Q	N	E	I	U	H	V	L	C	B	W	O	X	P	K	J	N	D	A	P	X	T	S	Q				
11	Z	C	O	A	U	Q	T	L	E	R	F	P	S	J	Y	G	B	D	H	N	W	M	K	X	V	I					
12	O	M	F	O	V	N	A	C	Q	U	P	Y	E	R	Z	K	J	S	D	L	I	T	N	B	W	H	A				
13	B	X	O	V	F	N	K	G	E	L	D	S	T	I	M	K	P	U	J	C	W	Y	J	S	Q	U	H	Z	P		
14	K	O	R	E	I	M	B	T	F	D	V	A	O	W	N	C	Q	L	X	Y	J	S	Q	U	H	Z	P				
15	U	H	A	L	V	O	Q	Z	E	B	K	X	I	N	Y	D	M	J	F	N	T	S	C	G	P	R					
16	P	B	N	H	K	O	J	F	Z	M	Y	L	I	V	R	U	T	Q	S	C	X	G	N	E	A	D					
17	B	R	K	W	X	V	M	X	L	O	P	J	H	A	F	J	D	E	S	N	T	I	Z	Z	P	U	O				
18	N	G	U	B	X	D	E	A	K	I	Y	Z	L	W	J	H	O	M	S	T	V	C	R	Q	P	F					
19	C	R	O	W	V	B	F	D	E	M	H	I	U	P	S	Y	X	G	J	K	Q	T	Z	L	A	N					
20	F	E	W	I	Z	T	A	R	B	U	N	Y	Q	C	V	M	X	L	D	K	G	H	O	S	J	P					
21	L	V	K	P	O	U	Z	B	Y	S	A	M	C	T	X	N	E	R	O	H	F	W	I	L	V	E	B				
22	D	S	M	I	J	K	C	R	F	N	W	Q	O	P	A	T	Z	G	X	Y	U	N	L	V	E	B					
23	P	T	F	C	W	K	I	U	N	D	J	A	E	N	O	S	Z	Q	M	L	R	B	V	G	Y	X					
24	N	Q	D	P	U	V	T	X	N	M	L	E	Y	B	O	N	C	R	P	I	K	Z	G	J	A	S					
25		A	C	J	V	H	S		E	I	K	M		U	T	D		N	R	Z	L	X	F	B							
26	O	Y	B	L	D	M	F	V	Q	C	X	T	U	K	P	M	G	H	W	S	A	I	E	J	Z	R					
27	M	N	K	L	S	O	J	C	Z	V	T	H	P	X	D	U	E	F	B	G	I	A	Y	W	Q	R					
28	R	P	J	Q	L	K	A	Y	X	U	C	N	B	M	V	E	Z	W	I	O	S	H	F	D	G	T					
29	N	M	S	T	R	U	Z	O	I	Y	E	P	J	K	L	F	O	D	A	B	V	C	X	Q	W	H					
30	N	Q	D	I	O	J	R	Z	Y	C	E	M		L	U		N	A	V	S	X		P	F	H						
31	K	J	Z	S	B	E	C	M	O	L	R	P	N	O	F	W	Q	D	X	Y	U	N	M	T	V	I	A				
32	V	R	D	W	N	F	O	A	U	I	N	E	Z	L	S	Y	P	K	J	B	M	Q	X	T	C	O					
58	U	O	T	S	E	B	Q	V	H	M	R	Y	C	W	O	P	L	J	D	N	F	I	Z	X	A	K					
84	A	R	H	W	J	B	D	L	X	Q	M	U	G	F	E	T	C	V	N	O	K	P	Z	Y	S	I					

In the study of the motion of the wheels during the course of encipherment, it was observed that:

1. Each time a key was depressed, the outside wheel was uniformly displaced one position by the outer turnover pawl.
2. Each time the notch on the ring of the outside wheel reached a position opposite the middle turnover pawl, the second wheel was also displaced one position, by the middle turnover pawl, the next time a key was depressed.
3. Each time the notch on the ring of the second wheel reached a position opposite the inner turnover pawl, the second and third wheels were simultaneously displaced one position, by the inner turnover pawl, the next time a key was depressed.
4. The fourth (reflecting) wheel did not move at all in the course of encipherment, but could be set at any position by hand.

This is the type of motion which came to be known as commercial or non-cyclometric motion.

It was decided arbitrarily to designate as the A position the effective position of the outside wheel for the first alphabet. The exterior contact points of this wheel were then assumed to be lettered with the normal alphabet starting with "A" as the contact point opposite Q on the end wiring. Thus, to remove the effect of the constant end wiring from the first alphabet, both letters of the plain-cipher pairs would be converted from end wiring identities to the lettered contact point identities appearing opposite them with the wheel in the above position. In order to keep up with the progressive motion of the outside wheel, and, simultaneously, to retain the relative order of the arbitrary lettering of the exterior contacts of the outside wheel, it was necessary to advance the wheel one position for each successive alphabet. The actual conversion was made with two paper strips, one lettered with the normal alphabet the other with the QWERTZU sequence and manipulated so as to represent the above described motion of the outside wheel relative to the end wiring. Thus, the table of wheel circuits in Figure 32 represents, by pairing the normal alphabet at the top of the table with any line within the table, the couplings of the exterior contact points of the outside wheel in terms of the arbitrarily assigned normal alphabet to identify these contact points, for the 34 cipher alphabets tabulated in Figure 31.

TOP SECRET ULTRA

FIGURE 32

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
Q W E R T Z U I O A S D F G H J K P Y X C V B N M L
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

1 Q V M S Q O U P N A C K G J T E R I B D Z H X
2 M I J R E R E Z A S T Y V M O B M O K
3 M C W B U U Z M E V J A K R P G L E O Q I
4 W A P Y Q Z F I Z R O U V L C R J Y D M H A H S I
5 F S P Y V A K Y L O M I K Q J C N U B R E Z O H E
6 M A P P E V T N U C R B I S D X L O N J C Q Q A
7 M L A C U S P Y A Z R J V O I X F Q T R N
8 P G H A S L B J O H C F T W I Y Z V M A R N D F O
9 T D E C I U O F Y V P S X H L W Z M A O K Q N J R
10 Z Y O U S V C M T W O A H L Q P X I D F K R B A
11 G Y H L I A D F P E S T Q K O M N W H U Z C X
12 B A V N K S P I N E T X Y O U P L R C D N O Q
13 K O S B G M E P M A V I F U H Y J C Z O L X W Q T
14 O K H N M O T C I T B S S E D A Q T U L J H Z Y I W V
15 H V P G Z M D A S Y I F R U C X N J W O T Q K E
16 Q W K S V T P J I C Q R Y A G L M D T X E B U N H
17 H F E Z C B S A U X V Q O Y M T G R J M O K P D
18 Y J W S O T P B V M L U R I O E X N K C V A T
19 U O G Z Y J C K I P H I S M X R P M V A T M O E D
20 W P Z A L P N O R M S E J G N O I K V U A V Z C
21 Z O M E D S O Y R R X C T G O J F U T P K L H A
22 L O N H J W V D M E Z A I O N S U Q R O Y T C K
23 X M D C X M F Y T C O B U V Z S R J O O A I Q
24 O D S B O O W Z P T O U R A J E N C K M H Y I
25 H S N T M O A O C O C J V B D X R U
26 R V Y K X O U Z C S D P P O N M N A J T G S O E C H
27 Y X Q Z K T P U V V R O B T L G C M W H J S B A D
28 F E S Q B A R K T U N V Y X Z W D G C I J L P M O
29 D Q Z A M G F I N K J R E T S B O P M L Y X Y C
30 P P R E D O K L S G I V M F B C J A M V I T
31 I Z L N U T J O A G Y C R D H V S M Q F E P T O T B
32 F Y J Z S A I Q G C R N O L M T R K E P I W V U P D
33 H A Y O V L S J P H B F A Y D I X Z O N W X U Q C R
34 H K X P M O I T G U B C E I F D L S H H J Z A C H V

TOP SECRET ULYSS

By the time this process of stripping off the keyboard sequence had been performed on the first five alphabets, it became apparent that remarkable results were being obtained from this procedure. These phenomena may be found boxed in and encircled in the first five rows of Figure 32. The most obvious patterns produced by these phenomena are those involving the repetition of two outside contact point circuits between each pair of lines. Also columns 8 and 25 have identities in rows 1 and 5 which occur as identities in rows 2 and 3 of columns 17 and 6 respectively. The pattern of column 8 has an additional aspect in that the values in rows 3 and 4 were found in rows 4 and 5 of column 7. In fact, each pair of rows was found to contain vertical pairs which had occurred one row higher, and the first occurrence of 2 of these pairs formed the second and third letters of an AAB pattern.

From these manifestations, the following appeared to be valid conclusions regarding the structure of such a table:

1. The occurrence of a certain number of identical columnar patterns at one level insured that the same number of the same type of columnar pattern would occur at any level.
2. There would be a definitely homologous, or isomorphic, relationship between the identity of the letters in the recurrence of these columnar patterns on successive levels.
3. If carried far enough, an analysis of this isomorphism would adequately serve to segregate the several apparently identical columnar patterns into distinctive ones, each of which would reappear on successive levels and each of which would be isomorphically distinct from each other pattern starting at the same level.

This, based on the second foregoing conclusion, it was predicted that row 6 would develop so as to reproduce, somewhere in rows 5 and 6, two of the four vertical pairs which occurred in rows 4 and 5 of columns 2, 9, 11 and 26; that the column containing one of the pairs, which did not recur in rows 5 and 6, would be a pattern corresponding to column 25; and, that a column containing one of the pairs, which did recur in rows 5 and 6, would be a pattern corresponding to column 8.

However, this prediction failed to materialize. In fact, no

TOP SECRET

pattern was found to continue into row 6; there was not even one case of a double letter across rows 5 and 6. At this point, this fact was tentatively, and rather vaguely, assumed to indicate that the second wheel might have been displaced between enciphering positions 5 and 6. Accordingly, the stripping process was continued, and a new series of columnar patterns was found to develop, starting with row 6 and continuing through row 31. Again at this point the progression was broken, and a new series was found to commence in row 32. However, it was here discovered that the progression could be continued from row 31 back to row 6, that, in effect, any such progression was cyclic within the span of these 26 rows. This fact led to a fourth conclusion regarding the structure of such a table:

4. Once segregated, a series of isomorphic columnar patterns would have to embrace 26 rows and, in doing so, would be progressively found starting once on each of the 26 levels and occurring once in each column, thereby, forming a closed cycle within a span of 26 rows.

This cyclic manifestation was considered definite corroboration of a displacement of the second wheel between enciphering positions 5 and 6, and also between positions 31 and 32, since, with one exception (cf. the third element of the wheel motion, prec.), the second wheel remains stationary for 26 displacements of the outside wheel. From this point, the stripping process was continued as far as any plain-cipher equivalences had been recovered.

In Figure 32, two of the many obvious series of patterns in rows 6 through 31 have been encircled throughout the table. The first one is of the form KEKE, starting in column 3, line 6. The second is of the form A-Q-A-Q, starting in column 26, line 6. The first practical use, to which these columnar patterns were put, was the derivation of the remaining elements of incomplete patterns, thus, enabling the derivation of additional plain-cipher equivalences. Thus, using column 1 as a criterion, the following identities (repeated in homologous positions in all columns) were noted:

Z-U-Z—OHQHYU-Z—OH-Y-U—

However, columns 7, 12, 16 and 17 had some blanks in them which (as permuted below) should involve identities isomorphic with column 1:

TOP SECRET ULTRA

7 F-P-F-VL-V-UP-F-V-U-P-
 12 I-V-I-OF-FOV-I-F-O-V-
 16 G-Q-G-SVBVJ-Q-SV-J-Q-
 17 P-Z-Y-DEBGSZ-DB-S-Z-

It is obvious that these four columns in this alignment are isomorphic with each other and with column 1. Therefore, the isomorphism with column 1 may be completed in each case, to produce new wheel point pairings and new derived plain-cipher equivalences. A similar situation resulted from columns 6 and 9 (as permuted below):

6 T-Q-T-LILIAG-T-LIVI-Q-
 9 N-L-N-FIFTH-N-FIFTH-L-

Here, these two columns are isomorphic with each other and with column 1, except for the encircled letters, indicating a necessary correction in originally erroneously assumed plain-cipher equivalences. In such fashion, isolated blanks were filled in, and isolated corrections made, as the stripping process continued.

However, in the course of experimentation with the progression of the columnar patterns through the 26 rows in one cycle, a far more powerful manifestation was noted. A listing was made of the successive columns (in terms of the contact points of the outside wheel) in which the columnar patterns appeared on successive levels within the 26 row cycle, together with the letters involved in each recurrence of the pattern. So, in the case of the KEKE pattern in rows 6-31 (omitting the second vertical pair), the following series were formed:

Column: C E S M J R U O A H Z D Q B P V G L F I T N X W Y K

Pattern: K C E S M J R U O A H Z D Q B P V G L F I T N X W Y
 E S M J R U O A H Z D Q B P V G L F I T N X W Y K C

So, also, for the A-Q-A-Q pattern, the following series resulted:

Column: Z D Q B P V G L F I T N X W Y K C E S M J R U O A H

Pattern: A H Z D Q B P V G L F I T N X W Y K C E S M J R U O
 Q B P V G L F I T N X W Y K C E S M J R U O A H Z D

TOP SECRET ULTRA

Thus, it became evident that the progression of any columnar pattern, through the 26 levels of one cycle, involved all columns in the same cyclic order, only commencing at a different point in this cycle for each individual pattern; also, that the identity of the letters constituting any pattern progressed, on successive levels, through the same cyclic sequence. Furthermore, examination of the letters not involved in any obvious pattern revealed that when the columns were selected in this same cyclic order the series of letters on successive levels produced the same cyclic sequence. In short, all the elements of indirect symmetry were present; and by rearranging the columns of Figure 32 in the order of this cyclic sequence, a form of Vigenere table would result, wherein the index line and all diagonals would be cyclic repetitions of one fixed basic sequence. This Vigenere development of Figure 32 is shown in Figure 33 with the QWERTZU (keyboard) sequence permuted according to the basic sequence version of the normal alphabet.

Surprisingly, the corresponding basic sequence for the cycle of rows 32-57, when reconstructed in the same manner, evolved as another cyclic repetition of the previously recovered sequence. In fact, the basic sequence for every cycle, or partial cycle, over the span of the messages proved to be the same, differing only in the starting points for the diagonals in the square for each cycle. Thus, it became possible to completely generate the quasi-Vigenere square for each full cycle of the outside wheel from either the complete set of values for any row or from one value for each of the 26 different diagonals. In such fashion, the plain text was derived for the almost complete decipherment of the messages.

Up to this point, the primary purpose had been to design a method for automatically producing the cipher alphabets necessary to read all the traffic, without any consideration of the possibility of recovering the wiring of the machine used in enciphering this traffic. At this point, however, consideration was given to what mechanical or electrical aspects of the machine might have produced the phenomena which provided the means of generating the cipher alphabets.

It was then realized that the columnar identities, which constituted the nucleus for the observed patterns, were the manifestation of two or more parallel or equidistant circuits through the three inner wheels. For, the repeated wheel circuits (through the four wheels) were between the same pair of exterior contacts on the outside wheel; and, since the wiring within one

TOP SECRET ULTRA

FIGURE 33

QILRKWJVUDZOXGNBMSETYFAPCH
AHZDQBVPVGLFITNKNWYKCESMJRUO

1 LYXWVJVJBOAQRKZDHNMSSECTTIG
2 LFKWYIORPAHBOUCDQZIJMSSEVNT
3 WFKICYKTLUVH2PAOEQBDWJRJMSGX
4 WFKITEKCNFOGZDVAHASBPPYURJML
5 ~~FIWNTNSCEXIALDQGGZHMFPVBKOURJ~~
6 ZTAPXNDQGVRENHIQYWCCKFOSULJS
7 MDNHVWJQLGUSXZTBKXYECIAPOFR
8 UJQXZGYZRBFLOMWDNPNCKSETHVAI
9 TORBWDLKKUPIFAJYQXVEGCMSENZOH
10 ZNAUPIYQFCOVTHHRKKBWGSEJMXIDL
11 FDXHOVKBIEAGONTZUCPYLMSRJWQ
12 BIQTWZAGCPTSHLXNDQEVKFKJMURY
13 KPTBYDHLLEVNMZFWXQASGCCIRJOU
14 OCVNPKQZFSQXJDIYNBHMLETURA
15 HAEQXVGBDIDLMLWRQTKYFZJFSNOU
16 OZHSLSWGEPPQTJFYUBNCKKVDRIMXA
17 HADZMFFYLSVBNRIKOPXECQQUJW
18 YZHQDJIKFMGPXUTCADVWSELBONR
19 UKDZBQRTCIJLVWONEHGYMSFDAX
20 WOCQDPPBUNETRFGYAXSZLKMIVH
21 ZYAEQBQVPOXSNUICLKHWMDFCRJTG
22 LDKHSPBQVAVWMXOTFCZYJQIEURN
23 XFPQCZMVPLGHYJWANIEDKRBTSOU
24 QWIB&DJGVFLZKRYHXTSQCUPNMA
25 HAYTPSQRLGIFDCUKZWNMBEDVXJ
26 RZHKNVMBUFLT IQEODYXJPSAGW
27 YUDZCIGJPOIFNTBSAEQKWRVMHL
28 FKOQDENLRVATIXNPMHSRCYUQJZ
29 DICABQSYFUGHNTW XVJZMPEKOLR
30 UQTEHPBMKIOLEZXXNYWGRDJVSCAF
31 IOBNSZVPJCTAFDWWXKYLUGROVHE
32 ~~FQDZHYTFWINAGPLUVBRJSROCKXN~~
58 ~~MJROXKIESPLPNTQUCBYVGAHZWD~~
84 ~~WTVPLKDDZIQOCHYCANBXMREUSJF~~

TOP SECRET

wheel was constant, this meant that the circuit was completed through the same pair of interior contact points also. Therefore, the pairs of exterior contacts of the second wheel, which were opposite this pair of outside wheel interior contacts, were the same distance apart and were separated from one another by an interval equal to the advance of the outside wheel between recurrences of columnar identities.

This conclusion led to the realization that the recurrence of an isomorphism, on successive levels of the 26 row cycles, was produced by a constant pattern of circuits through the three inner wheels being completed through successive equidistant pairs of interior contact points on the outside wheel. This in turn led to the recognition of the recovered basic sequence as, actually, an expression of the relative spatial displacement of the current entering each of the exterior contacts of the outside wheel, by the wiring from these contacts to the interior contacts of that wheel, in terms of the original arbitrary lettering of these contacts.

The reason for this will become evident from Figure 34. Suppose the normal alphabet to represent the arbitrary lettering of the contacts of the outside wheel, and two pairs of points marked A-A' and B-B' joined by loops to represent two adjacent parallel circuits through the three inside wheels. Then, with reference to Figure 33 rows 1-5, one series of patterns is the progression of identical circuits: A to L, H to F, Z to L, and D to T. These may be represented schematically as in Figure 34, indicating that the interior contact points which are wired to the outside contact points A, H, Z, D pass successively across A of the right hand loop at the same time that the contact points which are wired to L, F, I, T pass across point A'. This situation recurs with the same pairs of interior contacts as they pass points B and B' of the left hand loop and produce the previously noted phenomena of repeated identities in successive rows for the first 5 rows of Figure 33.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

	A	H	Z		L	F	I	T
B	X	X	A		B'	X	X	A'

Figure 34

TOP SECRET ULTRA

Each of the two four-letter sequences thus schematically employed to produce the AA patterns noted in the first 5 rows of Figure 13 are portions of the basic sequence shown as the index line and the downward left-to-right diagonals of Figure 13. It therefore follows that, if the second wheel had not been displaced between rows 5 and 6, the full basic sequence could have been employed in the same fashion to produce AA patterns until the second wheel was displaced. This fact thus fixes the true span of the parallel circuits so that the two four-letter sequences will fall in their proper relative position in the basic sequence.

Thus, one version of the wiring sequence for the outside wheel would be (using the schematic representation from Figure 3a):

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
E S M J R U O A H Z D Q B P V G L F I T H W Y K C

Other versions of this wiring sequence would result from other than the two arbitrary hypotheses made in this case. If another letter in the normal alphabet were used to designate the effective starting position of the outside wheel, each letter of the two components of the wiring sequence would be advanced through the normal alphabet an interval equal to that between A and the letter selected. If the parallel circuits through the three interior wheels were assumed to be located elsewhere with respect to the outside wheel, a corresponding displacement would result in the juxtaposition of the interior and exterior sequences. However, having selected any combination of these two possibilities, a wiring sequence would be recovered which would be equivalent, in its relative effects, to the true wiring of the actual wheel involved.

Having discovered that, by stripping the effect of the end wiring off the cipher alphabets, it was possible to recover an equivalent wiring for the outside wheel, it was realized that the same effect would be produced by the second wheel, if the effect of the outside wheel were stripped out of the table in Figure 32 (and its extension through the succeeding cycles of the outside wheel).

Accordingly, the same arbitrary assumption for the effective starting position, and the lettering on the ring, was made for the second wheel as had been made for the outside wheel. This sequence was then assumed to be displaced one position to the left for each successive cycle of the outside wheel in order to retain the correct relationship in the designation of the contacts on the second

wheel, while the recovered equivalent wiring for the outside wheel was rotated cyclically to conform to the outside wheel motion. As was expected, the circuits through the inner two wheels, thus derived, were identical throughout the span of each cycle of the outside wheel. It was found, also, that five cycles of the outside wheel were sufficient to derive an equivalent wiring sequence for the second wheel. Figure 35 shows the second wheel, exterior contact point circuits (from Figure 32) for alphabets 1, 6, 32, 58 and 84.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	E	S	M	J	R	U	O	A	H	Z	D	Q	B	P	V	G	L	F	I	T	N	X	N	Y	K	C
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	A	Z	N	T	S	P	Q	X	V	Ⓢ	R	O	D	M	G	H	L	F	E	Y	J	Ⓢ	I	U	C
6	M	Ⓢ	X	F	P	D	J	R	Y	G	L	K	A	W	Q	R	O	N	T	S	V	U	N	C	I	Ⓢ
32	W	S	Z	O	I	H	G	E	U	Q	T	P	R	E	M	K	N	C	L	J	B	A	Y	X	D	
58	F	G	H	I	A	R	C	B	T	Ⓢ	Q	Y	Z	P	O	L	S	R	J	D	X	Ⓢ	V	M	N	
84	D	Ⓢ	E	A	C	Q	V	S	N	M	P	X	J	I	R	K	F	O	H	W	Y	G	T	L	U	Ⓢ

Figure 35

	N	Z	A	N	D	F	I	E	C	M	R	U	Q	T	X	P	S	Y	O	H	J	L	V	K	B
1	Ⓢ	C	B	D	N	S	X	T	Z	O	L	Y	H	P	E	I	G	F	U	M	Q	V	R	J	Ⓢ
6	N	Ⓢ	M	N	F	D	Y	P	K	A	H	V	O	J	S	C	E	T	I	Q	R	O	K	U	Ⓢ
32	A	D	N	R	Z	I	F	O	S	P	N	J	K	H	L	Y	M	C	X	E	G	U	T	R	Ⓢ
58	Ⓢ	N	F	Z	U	A	E	I	H	Y	S	D	L	B	J	V	O	R	M	P	C	T	Q	X	Ⓢ
84	T	Ⓢ	D	I	A	Q	N	C	E	J	O	Y	F	V	N	L	K	H	U	R	S	M	X	G	Ⓢ

Figure 36

In Figure 35 the beginnings of a pair of columnar patterns are encircled. From the previous development of Figure 33 it is obvious that it was necessary only to pair correctly either column containing the pattern between rows 1 and 58 with either column containing the pattern between rows 6 and 84. From this correct pairing, the development of Figure 36 easily follows by anagramming the columns of Figure 35 so that any diagonal sequence is reproduced on the index line and vice versa. Thus, the basic cyclic sequence was reconstructed and, therefore, an equivalent

TOP SECRET ULTRA

wiring sequence for the second wheel would be (according to the representation of Figure 34).

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
V I A N D F I E C H R U Q J T Y P S T O N J L V K S

In the process of generating the cipher alphabets for the latter part of the decipherment (i.e., extending Figures 31, 32, 33) it was found a very difficult procedure to derive enough values on different diagonals (of Figure 33 extended) to generate the full table for the cycle starting with the 162nd letter of each message, from which point the maximum depth was 14 messages. However, having recovered the equivalent wiring for the outside and second wheels, this procedure was simplified by representing the wiring for these wheels on sliding strips, displacing them according to the relative motion of the two outside wheels in the course of encipherment with the machine. The combined effect of the two inner wheels, when derived according to the relative juxtaposition of the two outside wheels at any point in the span of the messages to this point, was found to be constant (i.e., the third wheel had not yet been displaced from its initial effective position). Thus, the resultant effect of the two inner wheels was represented by a third strip used to complete the schematic representation of the electric action of the machine at any point. Figure 37 shows one version of such a set of strips for the 162nd position of the messages. The encircled letters indicate the paths of the current from W on the keyboard (or the lightboard) to R on the lightboard (or the keyboard) when the wheels are in this relative juxtaposition. In this manner the decipherment for this cycle (positions 162-187) was completely derived.

This same procedure was applied to the next cycle (positions 188-213), but the resulting decipherments were unintelligible from position 189 on. It was thereby established that the third element of the motion had been effective between positions 188 and 189. However, the depth at this point had been reduced to five and it was thus impossible to establish enough values beyond this point, either to generate an additional cycle in the extension of Figures 31, 32 and 33 or to derive completely a resultant for the new juxtaposition of the two inner wheels.

TOP SECRET ULTRA

	Q	W	E	R	T	Z	U	I	O	A	S	D	F	G	H	J	K	P	Y	X	C	V	B	N	M	L
Outside Wheel	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	U	O	A	H	Z	D	Q	B	P	V	W	L	F	I	T	N	X	Y	K	C	E	S	M	J	R	
Second Wheel	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	E	C	M	R	U	Q	G	T	X	P	Y	O	H	J	L	V	K	B	N	Z	A	N	D	F	I	
2 Inner Wheels (Combined)	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Y	I	Z	E	D	R	P	O	B	T	W	S	U	Q	H	C	N	F	L	J	M	X	K	V	A	C

Figure 37

From the equivalent wiring of the two outside wheels, as recovered in this office, the Signal Corps identified these wheels as the actual ones furnished in the old Commercial Enigma Machine (Lot A-766) and the Navy later identified the traffic as that of the Swiss Army. The wheel order used for this traffic with respect to the numbers on the actual wheels was 1-3-2 (left to right, as one faces the machine).

RECAPITULATION

Although the wiring recovered in this solution later proved to be known wiring, this recovery of wiring assumed to be unknown was achieved without prior knowledge of any solution or technique for the recovery of Enigma wiring and is believed to be the first instance of Enigma wiring recovery in the United States. It should be noted, however, that the initial approach to the problem, i.e., the conversion of the end wiring identities to their exterior contact point equivalents on the outside wheel, was an adaptation of the procedure earlier used in the solution of the Hebern machine.

Refinements in, and improvements upon, the technique herein described have been made, resulting in more powerful approaches to the problem. Such refinements have established less cumbersome methods for deriving the equivalent wiring for each wheel. It has also been demonstrated that considerably more than the minimum number of couplings necessary to solution were utilized in this wiring recovery. Finally, at the time of this solution, the manifestations of "twist" were not fully appreciated. Hence, the recovered wiring was not recognized as that of the Commercial machine at hand.

TOP SECRET ULTIMA

PART II, C. ENIGMA: WHEEL WIRING UNKNOWN

2. MULTIPLE TURNOVER. GREEN MACHINE

a. HISTORY

A station using the call TQI2 was first heard on 10 October, 1942 on 10,415 kilocycles at 2114 GMT. This station sent calls up to 30 October, 1942 when a message was intercepted. Message preamble was 2910/301/66. TQI2 was believed to be linked with a station on 11,310 kilocycles using call TIM2 which was on the air between 1900 and 0320 GMT. On 12 November, 1942 it was learned from bearings taken by the FCC that TQI2 was in Europe and TIM2 was in South America. On 17 November, 1942 at a Radio Intelligence Meeting, RSE reported that TQI2 on 11,510 kilocycles was in Cologne, and TIM2 on 11,300 kilocycles was probably in South America. RSS 1/29, Hamburg to Bordeaux (Coast Guard 4-I) had discussed this service in traffic which was being read by GC & CS and Bordeaux was instructed to monitor and help in case of difficulty. Station TQI2 used the call RSE also. RSE was believed to be the alternate control from Bordeaux.

b. SOLUTION

During October and December, 1942, 28 messages were intercepted from the station TQI2. This series of messages had several duplicate message numbers, (2 315's, 2 316's, etc.). The messages were superimposed and tested for coincidences but, in spite of several striking repeats at the beginnings of messages, the coincidence was rather poor. The test was definitely above random however and it was assumed that most of the messages were enciphered with the same key but that the duplicate message numbers was possibly evidence of two different keys.

Accordingly it was decided to put all the messages together and attempt to solve them in depth, bearing in mind that perhaps only one of each duplicated number would solve and that the other would not yield intelligible text.

Actually, however, all the messages turned out to be enciphered with the same key. Upon solution it was discovered that the low coincidence test was caused by the fact that several practice messages were included in the series. These practice messages contained a short portion of plain text at the beginning and were filled out to average length with dummy text.

TOP SECRET ULTRA

With the messages superimposed the following frequency tables were compiled on the first 15 columns:

Col. 1	Col. 2	Col. 3	Col. 4	Col. 5	Col. 6	Col. 7	Col. 8
A 1	A 3	A 1	A	A 2	A	A	A
B 1	B 2	B 1	B 2	B 2	B 2	B 2	B 3
C 1	C 2	C 2	C 2	C 2	C 2	C 2	C 3
D 1	D 2	D 2	D 2	D 2	D 2	D 2	D 3
E 2	E 1	E 3	E 5	E 1	E 1	E 1	E 1
F 1	F 7	F 4	F 1	F 5	F 2	F 3	F 1
G 1	G 3	G 1	G 1	G 1	G 1	G 1	G 5
H 2	H 1	H 1	H 1	H 1	H 1	H 1	H 1
I 3	I 1	I 1	I 1	I 1	I 1	I 1	I 1
J 3	J 1	J 1	J 1	J 1	J 1	J 1	J 1
K 3	K 1	K 1	K 1	K 1	K 1	K 1	K 1
L 3	L 2	L 1	L 1	L 1	L 1	L 1	L 1
M 2	M 1	M 1	M 1	M 1	M 1	M 1	M 2
N 1	N 1	N 1	N 1	N 1	N 1	N 1	N 2
O 4	O 1	O 1	O 1	O 1	O 1	O 1	O 2
P 1	P 1	P 1	P 1	P 1	P 1	P 1	P 1
Q 1	Q 1	Q 1	Q 1	Q 1	Q 1	Q 1	Q 1
R 1	R 1	R 1	R 1	R 1	R 1	R 1	R 1
S 1	S 1	S 1	S 1	S 1	S 1	S 1	S 1
T 1	T 1	T 1	T 1	T 1	T 1	T 1	T 1
U 2	U 1	U 1	U 1	U 1	U 1	U 1	U 1
V 1	V 1	V 1	V 1	V 1	V 1	V 1	V 1
W 1	W 1	W 1	W 1	W 1	W 1	W 1	W 1
X 3	X 2	X 1	X 9	X 1	X 1	X 1	X 4
Y	Y	Y	Y	Y	Y	Y	Y
Z	Z	Z	Z	Z	Z	Z	Z

TOP SECRET ULTRA

Col. 9	Col. 10	Col. 11	Col. 12	Col. 13	Col. 14	Col. 15
A 2	A 1	A 4	A 1	A 8	A 3	A 2
B 1	B 2	B 2	B 1	B 1	B 3	B 1
C 1	C 1	C 3	C 1	C 3	C 3	C 1
D 1	D 1	D 3	D 1	D 2	D 1	D 2
E 4	E 3	E 3	E 3	E 2	E 1	E 2
F 1	F 1	F 3	F 2	F 2	F 1	F 2
G 1	G 1	G 4	G 1	G 1	G 1	G 2
H 1	H 1	H 3	H 1	H 3	H 2	H 1
I 1	I 1	I 1	I 1	I 1	I 1	I 1
J 1	J 1	J 1	J 1	J 1	J 1	J 1
K 1	K 1	K 1	K 1	K 1	K 1	K 1
L 1	L 1	L 1	L 1	L 1	L 1	L 1
M 1	M 1	M 1	M 1	M 1	M 1	M 1
N 1	N 1	N 1	N 1	N 1	N 1	N 1
O 1	O 1	O 1	O 1	O 1	O 1	O 1
P 1	P 1	P 1	P 1	P 1	P 1	P 1
Q 1	Q 1	Q 1	Q 1	Q 1	Q 1	Q 1
R 1	R 1	R 1	R 1	R 1	R 1	R 1
S 1	S 1	S 1	S 1	S 1	S 1	S 1
T 1	T 1	T 1	T 1	T 1	T 1	T 1
U 1	U 1	U 1	U 1	U 1	U 1	U 1
V 1	V 1	V 1	V 1	V 1	V 1	V 1
W 1	W 1	W 1	W 1	W 1	W 1	W 1
X 1	X 1	X 1	X 1	X 1	X 1	X 1
Y 1	Y 1	Y 1	Y 1	Y 1	Y 1	Y 1
Z 1	Z 1	Z 1	Z 1	Z 1	Z 1	Z 1

Plain text assumptions were then made and filled in tentatively in the order shown in the 6 following work sheets.

From the point shown on work sheet No. 6 the text was expanded to 40 positions in each message. This was relatively simple since the messages followed the known style and was made even simpler by the occurrence of "lobsters" in positions 5-6, 7-8, 13-14, 17-18, 23-24, and 31-32.

TOP SECRET ULTRA

WORK SHEET NO. 1

301 OHNHKWPYFTBQJET
BEST

302 VHWXHVDFETQMT
E T E

303 KCAMZDORMEZMPCE

304 UIVJKVVJTEZMHP
E

305 LKUEKWQGSXICPAK

306 OHODJXMFTSKYVFN
BE

307 FIGHGHIJLESFZTH

308 OHDDHNORDXLBOCL
BE

309 KYOXOVMPQFFAUT
T E

310 LDBXMMENMWJOTPK
T

311 VHWXHV-HWABUJKD
E T E

312 BAUCHVCUURWDARA
O E

313 MLHXQVMWKKCEIAX
ST E

314 HAUESVKLLQBHAZQR
E

315 YCUKDJIDMDIXLQJ

315 OHNHKWPYFTBQJET
BEST

316 JZGFRCDCFMATED

316 CDRX^TMWPYFXIDERA

317 WAUCUV^EKCLFJHOFZ

317 YJWNBDORMEZKEXD

318 LOGNLLMJOXSKOPT

318 YPVQDYHUNXCDJQB
E

319 FIDHOINUWBFCCG

320 JFPIMNGJBXIIAZS

320 NMHHBBONNFJGATB
S

321 MHWHZHLWFNTUATE
E

322 DLOJHVNJTOYBAAZ
E

323 KYOXOVMPQFFU - - -
T E

Assumptions:

1. H cipher col. 2 - E plain.
2. V cipher col. 6 - E plain.
3. O cipher col. 1 - S plain.
4. H cipher col. 3 - S plain.

TOP SECRET ULTRA

WORK SHEET NO. 2

301 OHNKKWPIFTBQJZT
BEST
302 VHWXHVHDFETQMT
E T E
303 KCANZDORNEZNPCE
F
304 UIVJKVVJTEZNMRF
E
305 LKUEKWQGSXICPAK
306 OHODJXMFTSKYVPH
BER T
307 FIOGHMJLESFZTH
K
308 OHDDHNORDXLBACL
309 KYOXOVMPOQFFAUT
FORTSETZUNGX
310 LDBXNMENNWFJGTPK
T
311 VHWXHV-HWABUJKD
E T E
312 BAUCHVCUURWDARA
O E O
313 MIHXQVMFKXCEIAX
ST ET
314 HAUESYKLLQBHAZQRN
OE N

315 YGUKDNIDMDIXLQJ
315 OHHXMWPIEBBRAVS
BEST
316 JZGPARCDCFMAITD
316 GDRXWPFYFXIDERA
T
317 WAUCUVKCLFJHGFZ
E
317 YJWHBDORMEZKEID
318 LOGNLLMJOXSKGPT
T U
318 YFPQDVHUNXC DJQB
E
319 FIDHOIHUNWBFPGCC
K S G
320 JFPIMNGJBXIIAIZS
320 NMHHBEONNFJGATB
S
321 MHWZHHLWFNTUATE
E Q
322 DLOJHVNJTGYBAAZ
R E
323 KYOXOVMPOQFU ---
FORTSETZUNGX

Assumptions:

5. KYOXOVMPOQFU (309 & 323) - FORTSETZUNGX

301 OHHIKWPYFTBQJZT BEST	315 YCUKDAIDMDIXLQJ
302 VHWXHVHDFETQMKX E T E	315 OHHIMNFPYBBBRAVS BEST
303 KCAMZDORMEZNPCE F	316 JZGPARCDCFMAZD
304 UIVJKVVJTEZNMRF A E	316 CDRIMWPIFXIDERA OT
305 LKUEKNQGSXICPAK	317 WAUCUVXCLFJHGFZ I E
306 OHODJXNFTSKYVPH BERICHT	317 YJWHBDORMEZKEXD
307 FIGHGHMJLESFZTH KA X	318 LOGNLLMJOXSGFT T U
308 OHDDHNORDXLBOL I	318 YPVQDVHUNXCDJQB E
309 KYOXOVMPOQFFAUT FORTSETZUNG	319 FIDHOIHUNBFFCCG KA S Q
310 LDBXMMENNWJGTPE T	320 JFPIMNGBXIIAZS D
311 VHWXHV-HWABUJKD E T E	320 NMHHBEONNFJGATE S
312 BAUCHVCUURWDARA O E O	321 NHHZHHLWFNTUATE E X Q
313 MLHXQVMWKKCEIAX ST ET	322 DLOJHVNJTGVBAAZ R E
314 HAUESVKLLQBBHAZQRW I OE M	323 KYOXOVMPOQFUF-- FORTSETZUNGX

assumptions:

6. Message 306 begins with "BERICHT"
7. I cipher in col. 2 - A plain.

TOP SECRET ULTRA

WORK SHEET NO. 4

301 OHHXKWPYFTBQJZT BEST	315 YCUKDNIDMDIXLQJ
302 VHWXHVHDFETQMK ET	315 OHHXKWPYBBBRAVS BEST
303 KCAMZDORMEZNPCE F	316 JZGPNRCDCFMATZD
304 UIJVJKVVJTEZHMRP NA E	316 CDRIMWPFYFXIDERA OT
305 LKUEKWGQGXICPAK H	317 WAUCUVKCLFJHGFZ I E
306 OHODJXMFTSKYVPH BERICHT	317 YJWHBDORMEZKEID ER
307 FIOGHMJLESFZTH KA E X	318 LOGNLLMJOXSGPT T U
308 OHDDHNNORDILBOCL I	318 YPVQDQVHUNXCDJQB E
309 KYOXOVMPOQFFAUT FORTSETZUNGX	319 FIDHOIHUWBFPGCC KA ES G
310 LDBXMMENNWJGTPK T	320 JFPIMNGJBXIIA ZS D
311 VHWXHV-HWABUJKD ET	320 NMHHBEONNFJGATE UNSER
312 BAUCHVCUURWDARA O E O	321 MHWZHHLWFNTUATE E E X Q
313 MLHXQVMKXCEIAX ST ET	322 DLOJHVNJTGYBAAZ R E
314 HAUESVKLLQBHAZQRW I HOE M	323 KYOXOVMPOQFU--- FORTSETZUNGX

Assumption:

8. Message 320 begins with "UNSER"

TOP SECRET ULTRA

WORK SHEET NO. 5

301 OHHXKWPYFTBQJZT BEST	315 YCUEKDJIDMDIXLQJ E
302 VHWXHYHDFETQMKT E T E	316 OHSHXWPIYBBBRAVS BESHX
303 KCAMEDORMEZNPCE F	317 JZGPFRCDCFMATZD
304 UIVJKVJTEZHMRP NA E	318 CDRXWPIYFXIDERA OT
305 LKUEKWGQSSXICPAK EH	319 WAUCUYKCLFJHGFZ HIE ER
306 OHODJXMFTSKYVPH BERICHT	320 YJWHBBDORMEZKEID ER
307 FIGHGHMJLESFZTH KA E X	321 LOGNLLMJJOXSIGPT T U
308 OHDDHNORDXLBACL T	322 YPVQDYHUNXCDBJB E
309 KYOXOVMPQQFFAUT FORTSETZUNGX	323 FIDHOIHUWBFCCG KA ES G
310 LDBXMMENNWWJGTPK T	324 JFPIMNGJBXIIAIZS D
311 VHWXHV-HWABUJKD E T E	325 NMHHBSONNFJGATB UNSER
312 BAUCHVCUURWDARA O E E O	326 MHHZHHLWFNTUATE E E X Q
313 MLHXQVMWXXCEIAX ST ET	327 DLOJHVNJTGIBAAZ R E
314 HAUESVKLLQBHAZQRW WIEHOERTEN	328 KYOXOVMPQQFU--- FORTSETZUNGX

Assumption:

9. Message 314 begins with:

- (a) WIR HOEREN - rejected
- (b) WIE HOEREN - rejected
- (c) WIE HOERTEN - retained

TOP SECRET ULTRA

WORK SHEET NO. 6

301 OHHXKWPYFTBQJZT ERSTENSIX	315 YCUKDVIDMDIXLQJ E N S
302 VHWXHVHDFETQMKT DRITTENSX	315 OHHXMWPFYBBBRAVS ERSTENSIX
303 KCAMZDORMEZNPCE F	316 JZGPNRCDCFMATZD S
304 UIVJKVVJTEZHMRP NA EE	316 CDRXMWPFYFXIDERA ZWOTENSX
305 LKUEKWOQXSICPAK E HEN	317 WAUCUVKCLFJHGFZ HIE ER
306 OHODJXMFTSKYVPH ERRICHT	317 YJWHBDORMEZKEXD IER
307 FIGHGHMJLESFZTH KA E X	318 LOGNLLMJOXSGPT T U
308 OHDDHNORDXLBOCL ER ITW	318 YPVQDVHUNXC DJQB EN
309 KYOXOVMPOQFFAUT FORTSETZUNGX	319 FIDHOIHUWBFPGCC KA ES N G
310 LDBXMMENNWJGTPK W T	320 JFPIMNGJBXIIAIZ DE
311 VHWXHV--HWABUJKD DRITTE	320 NMHHBEONNFJGATB UNSER
312 BAUCHVCUURWDARA E TE O	321 MHWHZHLWFNTUATE RIE X Q
313 MLHXQVMWXXCEIAX ST ET	322 DLOJHVNJTG YBAAZ V R TE
314 HAUESVKLLQBHAZQRN NIEHOERTEN	323 KYOXOVMPOQFPU--- FORTSETZUNGX

Assumption:

10. Message 316 (CDRXM) begins with "ZWOTENS" which in turn leads to message 301 beginning with ERSTENSX, message 302 with "DRITTENSX", etc.

TOP SECRET ULTRA

COMPLETED WORK SHEET

[illegible]

COMPLETED WORK SHEET

1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0
 311 V H W I M V - H W A B U J K D O T M P O G V Y R A A U V I A O Z O J R W I Q M Z
 d r i t t e f o r t e x x b r o n n e t e f f e z i n o s e o c n d e r s y n
 312 B A U C H V C U U R W D A R A Q U C P D I D C H I V B I P C E J A R P B X I Y D
 v i e r t e x f o r t e s e t z u n g x z e r s e t s e n z m o n o t i g e r w o
 313 M L H I Q V M W K X C E I A X R O T O G I Y P L E N A K B Q I R B F W E Y I E K Y
 b e s t a e t i g e n f u n k e t i l l e z e r b i t t e n i n r e r s o f t e
 314 H A U E S V K L L Q B N A Z Q R W P J K O W Q Y I C C V Q Y P E O L R A B X D U
 w i e h o e r t e n e i e z n e e r e o n n t a g e s e o n d u n g e n f o r e
 315 Y C U K D W I D M D I X L Q J L H X Y K V L J R Q H B H U H Q M I V D B Q S V A
 x u e b u n g e s p r u q u i u n v e r q l u e s e l t x x x x x
 316 O H H X M W P Y B B B R A V S O V B B X Y K C R B Q B F W K - Y J R R K T Z J P
 e r s t e n s x d a s b e s t e h e n d e s e n d e r s o l l t o u n t e r
 317 J Z Q P W R C D C F M A T Z D Q W Z K M O P Q N S E H O A K X I Y P W Z Y I P K P
 a q t u n g x s p r u q u s u r u e b u n g x n i q t v e r a q l u e s e l t x
 318 C D A X M W P Y F X I D E R A E W F W - F I Q P L O C - U T E O Z R - W E U P D
 s w o t e n s x z e r s a t z e g e r a e t u n d e e - t s o t w t - F x d i e
 319 W A U C U V K L F J H G F Z S G K K L M I Q Q Q H W F T B Q W A R W E R Z L D
 h i e r d e r v e r e i n b a r t e u e b u n g e s p r u q u i e t n i q t v e
 320 Y J W H B D O R M E Z K E X I D D B X J M M D B L M T Y V N R C O K B F I Y O J Y
 x v i e r t e n e x x n a q r i q t e n b r i b g e r s o l l t e n k e i s e e

TOP SECRET ULTRA

c. RECOVERY OF WHEEL WIRING

The plain-cipher keyboard pairs were converted to wheel point pairings, assuming arbitrarily that the wheel started in position "A" in the first position of the message and advancing it to "B", "C", etc. for the second, third and following positions. Thus:

Position 1

Wheel
entry
points: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Keyboard
sequence: Q W E R T Z U I O A S D F G H J K P Y X C V B N M L

Position 2

Wheel
entry
points: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Keyboard
sequence: L Q W E R T Z U I O A S D F G H J K P Y X C V B N M

In position 1, above a W/H plain-cipher pair is converted to O/B wheel point pair, E/O to G/I, etc. (These plain-cipher pairs are taken from Figure 38 and were compiled from the completed work sheet.) In position 2 a Q/Z plain-cipher pair is converted to a B/U wheel point pair, etc.

The complete compilation of these converted values is shown in Figure 39.

TOP SECRET ULTRA

FIGURE 38

Position	Q	W	E	R	T	Z	U	I	O	A	S	D	F	G	H	J	K	P	Y	X	C	V	B	M	L
1		H	O			C	N			E	J	L	V	K	W	A	F	X	Y	Z	D	N	U	B	S
2	Z	D	L	H	K	Q	C	A	Y	I	W	B	R	V	T	X	O	P	U	J	F	M	N	E	
3	V	I	U	O			E	W	R		H	B	T	S		C		V	P	X	D				
4	F		H	C	K		P	D		J	I				E	S	B	U		T	R		K	M	N
5	A	N	H	B	H	F	D	K	S	Q	O	U	Z	L	T	C	I		J			R	W	E	G
6		N	V	G	D			A	L	I		T	M	R	X				H	E		W	F	O	
7		L	O	K	M			G	E		P			I	N		R	S		C	X	B	V	H	T
8	M	I	J	N	L	P	F	W	H		D	S	U		O	E	Z	X	Y	V	C		R	Q	T
9		A	L		N		O		U	W	M	B	X	K		G	C		F	P		D	T	S	E
10	N	S	X	F	U		T	G		B	W	P	R	I		D		E		A	Q				
11		T	J	I	W	X	M	R		I	B		G	F	Y	E	V		H	Z	N	K	S	C	U
12	A		F	B	G		X	H	Y	Q	D	S	E	T	I		N		O	U	V	C	R	K	
13	L	C	A	V	Z	T	I	U	P	E	M		N	X		O		J	W	R		O	S	Q	
14	X		C	T	R	U	Z	K		N	V		B	P		I	Q	U	Q	E	S	F	A		
15	N	B	H	D	S	A	J	L		Z	T	R		C	E	U	X	V		K	G	P	W	Q	I
etc.																									

etc.

TOP SECRET ULTRA

FIGURE 39

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1 -	O	I	U	X	C	P	Z	V	Q	B	J	M	T	S	F	L	Y	G	W	K						
2 -	D	O	N	A	P	B	V	K	T	I	C	X	E	W	U	J	S	H	Q	N	Z	Y				
3 -		J	I	K	P	E	D	F			Q	Y	G	M												
4 +	B	A	P	K	W	U	O		S	K	D	N	Z	J	H	O					T					
5 +	N	F	G	R	N	B	C	A	S	Q	P	U	O	E	M	K	J	D	I	Y	L					
6 +	N	F	G	R	N	B	C	A	S	Q	P	U	O	E	M	K	J	D	I	Y	L					
7 +	Z	C	B	U	K	H	L	F	O	W	E	G	Y	T	I	V	X	S	R	N	D	P	J	Q	M	A
8 -	Z	C	B	U	K	H	L	F	O	W	E	G	Y	T	I	V	X	S	R	N	D	P	J	Q	M	A
9 -	U	Z		T	M	S	K		L	H	J	F		Q	O		G	E	B	Y		V	G			
10 +	U	Z		T	M	S	K		L	H	J	F		Q	O		G	E	B	Y		V	G			
11 -	F	I	P	H	A	U	E	Q	T	O	Z	R	L	D	I	N	J	O		X	W	G	M			
12 +	I	T	R	O	F	O	B		U		X	H	Y	E	Z	D	L	W	V	N	P	S				
13 -	E	F	U	A	B	N	P	X	Z	W	M	L	O	V	H	R	Q	T	S	D	O	K	I	C	J	
14 +	E	F	U	A	B	N	P	X	Z	W	M	L	O	V	H	R	Q	T	S	D	O	K	I	C	J	
15 -	I	Q	U	N	J	E	B	F	P	O		V	L	K	C	Z	Y	X	D	N	T	S	R			
16 +	W	F	R		B	U	L		T	O	X	M	V	Y	C	Z	K	O	P	A	N	Q	S			
17 -	C	J	A	U	L	I	Z	X	F	B	T	E	W	P	O	M	S	R	K	D	Y	N	H	V	O	
18 +	C	J	A	U	L	I	Z	X	F	B	T	E	W	P	O	M	S	R	K	D	Y	N	H	V	O	
19 -	T	E	C	U	Y	L	Q	J		P	O	K	V	B	H	S		Z	I	X						
20 +	C	X	A	J	M	P	Z	D	T	E	W	U	F	R	Q	V	K	O	S	N	B	H				
21 -	E	H	A	Z	Y	C	N		W	J	U	S	Q	X	P	M	T	O	F							
22 +	V	N	I		L	Y	Q	C	R	F	O	B	M	H	K	W	X	Z	A	S	T	O	U			
23 -	Z	P	L	S	U	K	Q	X	O	M	F	C	J	R	I	B	G	N	D	W	E	Y	T	H	V	A
24 +	Z	P	L	S	U	K	Q	X	O	M	F	C	J	R	I	B	G	N	D	W	E	Y	T	H	V	A
25 -	X	Z	F		C	R	Y		W	N	M		H		V	U	L	A	I	B						
26 +	Y	D	B	U	I	G	N	Z	T	J	S		P	M	E	W	V	A	K							
27 -	J	R	W	S	Q	T	I	Z	A	U	P		M	E	B	D	F	K	Y	C	O	V	H			
28 +	P		M	O	N	X	T	Y		W	C	E	D	A	S	Q	H		L	F	I					
29 -	R	E	M	C	L	I	O	Y	Z	F	D	O	N	X	B	V	T	Q	J	K						
30 +	V	X	G	Z	P	M	C	I	N	U	L	K	F	T	Y	E	W	N	J	A	R	B	O	D		
31 -	T	U	Y	X	M	L	V	S	N	H	O	K	R	Q	P	O	J	B	C	I	E	D				
32 +	T	U	Y	X	M	L	V	S	N	H	O	K	R	Q	P	O	J	B	C	I	E	D				
33 -		T	K	V	Y	L	W	S	E	H	X	Z	U	N	P	J	D	O	F	I	M	O	N			
34 +	C	A	E	D	N	U	O	J	I	L	K	F	H	R	Q	W	O	S	Z	X						
35 -	T	N		J		O	F	L	K	R	S	I	Z	M	N	B	Y		U	P						
36 +	T	N		V	N		R	M	Q	K	C	Z	L	J	G	B	E	F	Y	X	P					
37 -	L	R	M	X	S	N	O	U	N	B	D	K	H	Y	C	F	J	F	E	Q						
38 +	K	O	I	T	F	C		X	S	E	Q	P	W	N	G	Z	Y	R	M	V	U					
39 -	O	Q	N	O	F	L	K	S	I	H	E	B	R	C	P	J	Y	I	Z	V	T	W				
40 -	T	U	G	X	E	L	M	R	H	I	S	Y	Z	K	N	A	C	Y	P	Q						

TOP SECRET ULTRA

Figure 39 was examined for equidistance patterns and the following was selected for examination:

Position		1	2	3	18		2	3	4	19
(N	Q	C	Q	--Q	F	R	K	R	--R
Letter (Q	N	N	N	--N	R	F	F	F	--F

This pattern was accepted as evidence that either wheel entry points NF and QR or NR and QF were wired to consecutive positions on the interior face of the wheel. Both situations were examined as follows:

TOP SECRET ULTRA

The pairings produced in positions 5-6, 7-8, 13-14, 17-18, 23-24, and 31-32 were stricken out because of the known turnover in these "lobster" positions and both arrangements were examined for repeated pairings. The MF - QR arrangement indicated nothing significant but the MR - QV arrangement showed the repeated pairings OS, WK, JN, CB, DW, RJ, IM, YI, and SL in addition to the MR and QV already assumed.

These pairings were added to the MR and QV in the table shown below, in which the repeated A-Z sequence replaces the position numbers. This table was then examined and positions that showed agreement with the assumed correct pairs were taken to be non-turnover positions, and positions which showed definite conflicts within themselves or with the assumed correct values were taken to be turnover positions and stricken out as shown.

TOP SECRET ULTRA

The pairs from the correct positions in the above table were then chained to produce the following sequence:

A T O S L Z E X M R J H N Q F D W K P V Y I G C B U

This sequence is an equivalent of the outside wheel points which are wired to successive points on the interior face of the wheel. It was then arbitrarily placed with "A" against "A" to represent the wheel wiring, as follows:

Inside:	A T O S L Z E X M R J H N Q F D W K P V Y I G C B U
Outside:	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

The above representation is intended to indicate that point "A" on the outside of the wheel is wired to the inside point where "A" appears, outside point "B" to the point where "B" appears on the inside of the wheel, etc.

With the wiring recovered for the first or outside wheel a conversion table was prepared for the second wheel, which was also arbitrarily assumed to start in the "A" position, as follows:

Wheel 2	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
	A T O S L Z E X M R J H N Q F D W K P V Y I G C B U
Wheel 1	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Figure 39 indicates that B and O wheel points are connected in position 1-3 of the text. These points are taken through the outside wheel placed against the second wheel at the above juxtaposition and converted to G/I; G/I are connected in Figure 39 so they are taken through the outside wheel and converted to I/V, etc. This procedure was continued, moving the outside wheel 1 step per position of cipher text and advancing the second wheel as indicated by the wheel track. The complete table of this conversion is shown in Figure 40. The letters at the left of the figure show the position of the second wheel and the numbers at the right show the number of positions in the text that the wheel remained stationary at the indicated position.

TOP SECRET ULTRA

FIGURE 40

ABCDEFGHIJKLMNOPQRSTUVWXYZ

A	JDIYBTRLWNASGPIZMUFKEQXHVCO	1-4
B	SWNJQZMKXIDHVGCPORXAUTLBIRF	5
C	SWNJQZMKXIDHVGCPORXAUTLBIRF	6-7
D	SWNJQZMKXIDHVGCPORXAUTLBIRF	8-10
E	FKZGVADPUMBNJLRHTOXQIEYSWC	11-12
F	OXGYLPCRSKJJEVQAFNNHIZWMUBDT	13
G	OXGYLPCRSKJJEVQAFNNHIZWMUBDT	14-17
H	OXGYLPCRSKJJEVQAFNNHIZWMUBDT	18-20
I	YRTQWXMJKNHIZSGUVDBMCOPEFAL	21-22
J	JEQOBLHGPARFTSDICKNNMYXZVUW	23
K	JEQOBLHGPARFTSDICKNNMYXZVUW	24-26
L	OIKTFEPFSBUCVZXAGWYHNDJLQHRM	27-30
M	VDXBQHJFWORSTYPOEKLMAZICNU	31
N	VDXBQHJFWORSTYPOEKLMAZICNU	32-33
O	FIRGHADEBSXYZWPOUCJVQTNKLM	34-35
P	FVOJPAKQTDOMLUCEHWZINBRYXS	37-38
Q	SRO YCOPUQX HIKBA JZNLFPV	39
R	KC BFE QPRA ZV IHJ NY WM	40

TOP SECRET ULTRA

The first 6 different sequences from Figure 40 were superimposed as shown in the table below and "chained" vertically to produce the chains indicated:

```

1 JDIETRLWNASGPITZMUFKEQJHVCQ
2 SWNSJQZMKXDRVGCPOEYAUTLBIRP
3 FKZGVADPUNBNJLRNTOXQIEYSWC
4 OKGYLPCKRSKJEVQAFPHIZWNUBDT
5 XRTQWXNJKHIESGUVDBMCOPEFAL
6 JEQOBLEGPARTTSDICKSMYXZVUK
  
```

1-2 JSNB (J) DWKA (D) YNXLMOF (Y) TQ (T)

UE (U) RZPGVIC (R)

2-3 SFCLETI (S) WKPR (W) NZAXUQV (N) JO (J)

ND (N) NBYO (N)

3-4 FOH (F) KXIWDCTHEM (K) ZOYUSBJVLQ (Z)

APR (A)

4-5 OYQGT LW (O) XRJIMP (X) CND AUEZ (C)

SKNBVV (S)

5-6 YJOSTQO (Y) REZFVI (R) WDKPXL (W)

NNAUDCM (N)

The symmetrical chains produced by chains 1-2, 2-3, and 4-5, 5-6, indicated that these two sets of chains were produced in three successive placements of wheel 2 against a combined Unkehr-walze and third wheel while the relative juxtaposition of the latter two remained constant. Accordingly equal length chains of 1-2 were slid against 2-3 chains and each juxtaposition checked for conflict or confirmation by superimposing similar pairs of letters in the 4-5 and 5-6 chains. This produced the following set of confirmed juxtapositions.

```

1-2 DWKA JSNB YNXLMOF TQ U RZPGVIC
2-3 ONBY RKP UQVNZAX ND JO 13FCLET
  
```

```

4-5 OYQGT LW NDAUEZC XRJIMP FVSKNB
5-6 AUDCMNM QOYJOST VIREZF XLWDBP
  
```

TOP SECRET ULTRA

The vertical pairs resulting from the above are combined to form the following sequence, which represents an equivalent of the sequence of outside wheel points on wheel 2 which are wired to successive points on the inner face of the wheel:

ATUJRIEGCTNZSWNEBPFIVLNQDO

This sequence is again arbitrarily placed "A" against "A" to represent the wheel wiring for wheel No. 2, thus:

ATUJRIEGCTNZSWNEBPFIVLNQDO
 ABCDEFGHIJKLMNOPQRSTUVWXYZ

The recovery of wheel 3 followed the same procedure as for wheel 2. Wheel 3 was assumed to start at the "A" position and wheel 2 was placed against it as shown below.

Wheel 3 ABCDEFGHIJKLMNOPQRSTUVWXYZ

Wheel 2 ATUJRIEGCTNZSWNEBPFIVLNQDO
 ABCDEFGHIJKLMNOPQRSTUVWXYZ

Figure 40 indicates that A/J is coupled so this pair was taken through wheel 2 and converted to A/D on the outside of wheel 3. The E/D pair, from Figure 40, was converted to I/Q etc. Wheel 2 was advanced through the cipher text according to the position numbers shown at the right of Figure 40 and wheel 3 was advanced according to the couplings produced. If the couplings remained constant the wheel was considered to be stationary, if the couplings changed wheel 3 was advanced.

The complete table of conversion of wheel 2 couplings to wheel 3 couplings is shown in Figure 41.

FIGURE 41

ABCDEFGHIJKLMNOPQRSTUVWXYZ

A	DIXASWJVBORZPOMNYKEUTHFCQL	1-5
B	DIXASWJVBORZPOMNYKEUTHFCQL	6-7
C	DIXASWJVBORZPOMNYKEUTHFCQL	8-12
D	LNKMTOPJSHDACBRQPOIEVUZYXW	13
E	LNKMTOPJSHDACBRQPOIEVUZYXW	14-17
F	LNKMTOPJSHDACBRQPOIEVUZYXW	18-23
G	LNKMTOPJSHDACBRQPOIEVUZYXW	24-30
H	ISYOFEXIQANZTUJVDVHNBMLFRGCK	31
I	ISYOFEXIQANZTUJVDVHNBMLFRGCK	32-38
J	SADGNTSPSQXYUORMOIZHFLWVJKR	39—

TOP SECRET ULTRA

The first 4 different sequences from Figure 11 were superimposed as shown below and then chained vertically to produce the indicated chains:

1 D I X A S W J V H G R Z P O N M Y K E U T H F C Q L
2 L N M E T O P J S R D A C B R Q P O I E V U Z Y X W
3 I S Y O F E I Q A N Z T U J D V H W B L M P R G C K
4 B A D C H T P S Q X Y U O E N G I Z H F L W V J K R

1-2 DLWGHUEINR (D) XMQ (X) AKOBSTVJFZ (A)
PCY (P)

2-3 LIBJQVMYGE (L) NSATFXICUPH (N) KOW (K)
DZR (D)

3-4 ISH (I) SAQ (S) YDMLFNXPWZ (Y) OCKRVO
JETU (O)

Chains from 1-2 were superimposed on their counterparts in the 2-3 chains and checked for conflict or confirmation by superimposing similar pairs of letters in the 2-3 and 3-4 chains until the following confirmed result was found:

1-2 PCY XMQ L W G H U E I N R D S T V J F Z A K O B
2-3 D Z R W K O J Q V M Y G E L I B F I C U P H N S A T
2-3 N S A T F X I C U P H L I B J Q V M Y G E K O W D Z R
3-4 L F N X P W Z Y D M J E T U O C K R V O S A Q B H I

The vertical pairs resulting from these juxtapositions were combined and placed with A to A against the normal alphabet to represent the wiring of wheel 3. Thus:

Inside: A N L J U Y R I E G V C Z H M K S F P D B T X W Q O
Outside: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Wheel 3 was then juxtaposed against the normal alphabet representing the Umkehrwalze, which was assumed to start in the "A" position; and the wheel point couplings from Figure 11 were then taken through wheel 3 and converted to Umkehrwalze couplings. Thus:

T Z M J V Y P U Q D N W C K S O I X O A H E L R V B
Umkw: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

TOP SECRET ULTRA

Wheel 3 A N L J U Y R I E G V C Z H M K S F P D B T X W Q O
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

In the above notation for the Umkehrwaise, T/A means that entry point "A" is looped to entry point "T", R/Z means that entry point "R" is looped to entry point "Z".

In completing the reading of the series of messages the following turnover pattern was found:

Wheel 1 A B C D E/F G/H I J/K L/M/N O P/Q R/S T/U V/W/X Y Z/

Wheel 2 A B/C/D E/F G/H I J/K L/M/N O P/Q R/S/T U/V W X/Y/Z/

Wheel 3 A/B/C D/E/F/G H/I J/K/L M N/O/P/Q R/S T/U/V/W X Y/Z/

The turnover patterns of 11, 15, 17 had likewise been found on the Group II machine used by German agents in Europe and which had been solved by the British prior to the appearance of the 3-W circuit.

4. LATER DEVELOPMENTS

Upon completing the recovery of the wheel wiring for the Green Enigma, Rod Squares and Inverse Tables were prepared, and the compilation of a catalogue was begun. While the latter was under preparation, further solutions were achieved. On 11 January, 1943, messages were transmitted with external serial numbers 322 to 338. It was possible to align them in depth by stepping each successive message one position to the right, producing a 10-letter repeat in messages 322 and 327. After the first rapid success with assumptions for the beginnings of the messages the complete plain text was reconstructed.

STEPS IN THE SOLUTION OF MESSAGES 322 to 338

1. Assume that T cipher equals E plain in column 5
2. Tentative trials of common initial words with E in the fifth place in message 322 lead to ERSTENS which produced a reciprocal (W/S) in column 3 to suggest ZWOTENS in message 323, and (T/S) in column 4 for SECHSTENS in message 325.
3. VIERTENS in message 324.
4. SECHSTENS X in message 325. NR Y AQT X in message 326. NR X NRUN X in message 327. NR X KINS MULL X in message 328. NR X KINS KINS XX in message 329.

TOP SECRET ULTRA

5. Filling in values and assuming "lobsters" in successive positions suggested SPHUCH at beginning of message 333, with a lobster between columns 17 and 18.
6. X_2 equals X_7 in column 17.
7. ACHT in message 337.
8. Double lobster in columns 16, 17, 18.
9. UMFANG in message 327, column 15.
10. HINWELSE in message 330, column 15.
11. SIESTENS X in message 336, column 15.
12. ACHTENS X in message 337, column 16.
13. WIE GROSS in message 322, column 9.
14. BISHERRICH in message 322 and 327, columns 24, to 33 inclusive.
15. UMFANG DER BISHERRICH in message 323, column 10.
16. BISHIR in message 324, column 12.
17. UMFANG DER BISHERRICH in message 326, column 13.
18. WELKE in message 329, column 21.
19. IN WELCHEN in message 325, column 14.
20. WELKE in message 328, column 20.
21. ERSTENS in message 331, column 10.
22. WICHTIGES in message 335, column 18.
23. DREI KIMS in message 333, column 19.
24. DIESER AEMTLICHEN in message 338, column 17.
25. KINE in message 335, column 14.
26. ZWECKMAESSIGE in message 330, column 20.
27. UMFANG in message 325, column 23.
28. ENGFASSEE in message 329, column 26.
29. AERONAUTIC in message 336, column 24.
30. ERFOLOTE X IM GANGE in message 324, column 18, assuming garbles in columns 19 and 21.
31. FUENF in message 333, column 27.
32. JOINT ARMY in message 337, column 24, assuming garble in column 26.
33. MUNITIONS ASSIGNMENT in message 331, column 19, assuming garble in column 19.
34. STELLE FUER in message 335, column 26.
35. MUSTER in message 328, column 25.

TOP SECRET ULTRA

11'111111122222222223333
123456789012345678901234567890123

322 IIWSTORQZERRCKPELLRILPWTURTORUJMDG
erstenexvielgroesseindioberherigen

323 HSZEPGZENEDHCHQXIVPICTORPCHNAOAL
swetenexumfangderbisherigenzgoe

324 KRTGLRBDIFQDKWBVEBKXLYLUTMORAL
viertensxbishererfolgtoeingange

325 TTZKZKWAPVTLEIXJRUNHWWJVCVHMD
sechstensxiwleichenumfangeerge

326 UOCNCJIWHTOJJZQKAWLJCAVHRRV
erxaqtxumfangderbisherigenx

327 OSQBWHOVHCKZMIZPSFURTORUJMDG
erxneunxxumfangderbisherigen

328 GEEWIOBCGSSKHMURFOAPPNVMVTJY
erxeineenullxxwelqemustervur

329 OVVRNADSBJOMYMSJDICVCFGOIF
erxeineinsxxwelqeenpaess

330 NRAXWTEWNJWOMSMJAJCWVJMDL
hinweiseaufweekmaessige

331 WEPFLLEKXAGVEPQQPKWNXAA
erstenexhmanitionsaassign

333 PJVCREDZHUWTPQTKJVSURV
spruchxdreieinsfuenfx

335 FDTXYNTPGWEITQRKTOMC
einewichtigestellefu

336 EBXHNQGECHIVHZZTZWVSU
siebtensxaeronautie

337 ZPBHQGEQAGJVMTHOLM
achtensxjoitv army

338 MRQOUXGASBVQROPP
diesesaentlichens

TOP SECRET ULTRA

The ring settings having been changed from those effective in the earlier messages, the wheel positions were found by inspection of the Red Squares. The wheel order was found to be the same as that for the earlier traffic.

Two later series of messages solved in depth were the means of discovering the method used on this circuit for the monthly ring setting and grandstellung. Eleven messages on 19 June, showing serial numbers 501 to 512 with 500 missing, were aligned by stepping to the right one place.

Repeated letters in 11th, 14th and 17th columns of messages 506 - 507 suggested the frequently appearing beginning, BOSS J, followed by a message serial number. Trial produced BO for another BOSS in message 509. These values were expanded as shown on work sheet below and values in a column were cataloged.

WORK SHEET OF MESSAGES 501 TO 512

		1 1 1 1 1 1 1 1 1 1
	1 2 3 4 5 6 7 8 9 0	1 2 3 4 5 6 7 8 9
501	B C F W V I N T G M U K N I M Y B H L	x b o s s j s i e b e n j x t u r s
502	N F I H T K F U X O F I P B W F P M	f o f o y d e r p r a e s i d e n t
503	I X H R H K Z I F O A Z L Z H L R	y b o s s j a q t j x a u s s e n
504	J W O B U X U V L S T Y E U L N	z y b o s s j n e u n j x b e r
505	I Y H K Y D E K N P B W Q Z N	f t s j n e u n j s i n d d e
506	N I O Q C B O M R T C R T N	x y b o s s j s e h n j a r
507	I Z L V B C M R U B R W M	y y b o s s j e l f j s t
509	A M S J U P Y S P Q A	z z b o s s d r e i z
510	P X G C P M W J N A	x y b o s s d r e i

TOP SECRET ULTRA

WORK SHEET OF MESSAGES 501 TO 512 CONTINUED

	1111111111
1234567890	0123456789
511	IOGPIYUOLN bbsajvief
512	RWYMZRBDW ybbsajfu

The position of the rings was recovered and all June traffic was read. By this time it seemed certain that the circuit was using a constant fixed wheel order.

Some early July messages were attempted on the June ring settings and starting point, since the encipherment date could very possibly have been the last day of June. The messages produced plain text with occasional garbles. This success led to the attempt to read further July traffic, and then it was observed that the "garbles" could be resolved by adjusting the ring on wheel number 2. Thus all July traffic was read.

Then on 12 August, six messages with serial numbers 568 to 573 inclusive were transmitted. These were solved in depth and the wheel positions found in the catalogue.

Trial of FTS at beginning of all messages produced -FTJ at beginning of message 570 and -FT at beginning of message 572. This suggested a repetition of the series of messages 540 to 546 mentioned in message 57b from Berlin to Argentina on 19 July, 1943. Trial of numbers 540 to 546 brought immediate confirmation as shown.

WORK SHEET OF MESSAGES 568 TO 574

	111111111122222222
	1234567890123456789012345678
568	IXBXHONFVPHLUMMBZLMJALJQMPTI rptjfuenfjvierjnulljbossjw
569	RSPVUMKVYWKKBDFMCA SRWMAJVR foforptjfuenfjvierjeinsjbo
570	UFHSEMOLDLIGZPYDACNOXWFL rptjfuenfjvierjsweljbossjd

TOP SECRET ULTRA

ONE SHEET OF MESSAGES 568 TO 574 CONTINUED

	111111111112222222222
1234567890123456789012345678	
571	PHJDQRHNDINQUARYIKHZNQGDSSV f t s r p t j f u e n f j v i o r j e r o i j b o
572	QVICPZGFIKPKJLQHCHVLUBH r p t j f u e n f j v i o r j v i o r j b o o s
573	FIBTIJLYVZZRSIGSITAOFFD f t s r p t j f u e n f j v i o r j f u e n f
574	EKQHQZBAFLFTLQHCHVBOXS f t s r p t j f u e n f j v i o r j f u e n

The rings were set in accordance with the convention first adopted for this machine - namely, using Z on the core as the zero point.

At this point the ring settings were examined for possible use of plain text words. The core identification normal alphabet sequence, arbitrarily assigned at the time of the original solution, was written out for all three wheels and under this sequence was written the correct juxtaposition of the ring for each of the monthly keys which had been solved.

Wheel 3		Core
	ABCDEFGHIJKLMOPQRSTUVWXYZ	
Jan:	CDPQHIJKLMOPQRSTUVWXYZAB	Ring
June:	KIYZACDEFGHIJKLMOPQRSTU	"
July:	WXYZACDEFGHIJKLMOPQRSTU	"
Aug:	KXYZACDEFGHIJKLMOPQRSTU	"
Wheel 2		Core
	ABCDEFGHIJKLMOPQRSTUVWXYZ	
Jan:	PQRSTUVWXYZACDEFGHIJKLMO	Ring
June:	PQRSTUVWXYZACDEFGHIJKLMO	"
July:	NOPQRSTUVWXYZACDEFGHIJKLM	"
Aug:	IJKLMOPQRSTUVWXYZACDEFGHI	"
Wheel 1		Core
	ABCDEFGHIJKLMOPQRSTUVWXYZ	
Jan:	KXYZACDEFGHIJKLMOPQRSTU	Ring
June:	KLAMOPQRSTUWXYZACDEFGHIJ	"
July:	KLAMOPQRSTUVWXYZACDEFGHIJ	"
Aug:	KXYZACDEFGHIJKLMOPQRSTU	"

TOP SECRET ULTRA

The columns were then examined for possible combinations to produce plain text. The Y columns of all wheels were eventually selected and combined to produce,

U 3 2 1

A N U
U N I
U L I
U G U

suggesting that the name of the month was being used for the ringstellung. It seemed quite odd that the rings should have been set opposite Y on all wheels but it was decided to try the ring set at Y on the Umkehrwalze also and to step the machine back to the point of origin to find the grundstellung for each key. It was known at this time that the starting point for each message was determined by stepping the machine forward from a basic starting point a number of steps equal to the last 2 digits of the number appearing in the message preamble. It was thus found out that the basic starting points were:

	Ringstellung	Grundstellung
January	J A N U	A R J A
June	J U N I	J U N I
July	J U L I	J U L I
August	A U G U	S T A U

Use of the same convention permitted reading of scattered unsolved messages on other months and all messages intercepted thereafter.

Later examination of the starting point used for the messages from which the wiring was recovered revealed that the Ringstellung used was Z Z Z Z and the Grundstellung was A A A A. A lobster was produced before the encipherment of the first letter of the text at which point the window reading was actually B B B B. This was the position which had been arbitrarily called A A A A in the wiring recovery and thus explains why it was possible to set the rings for all wheels at the core position arbitrarily designated as Y.

TOP SECRET ULTRA

PART II, C. ENIGMA: WHEEL WIRING UNKNOWN

3. RED MACHINE

a. HISTORY

The first mention of this machine appeared in message No. 14- sent on the GREEN channel, enciphered in the GREEN Enigma which had already been solved by the Coast Guard,^{*} and was currently being read. This message read:

"The trunk transmitter with accessories and Enigma arrived v/a RED. Thank you very much. From our message number 150 we shall encipher with the new Enigma. We shall give the old device to GREEN. Please acknowledge by return message with new Enigma. LUNA."

On the same day, the RED section sent message No. 909 stating that an additional Enigma machine had arrived. This message was enciphered by the Kryha machine which had been solved by the Coast Guard and was currently being read.

On 5 November, 1943, Berlin sent message No. 585 to the GREEN section in Argentina, saying:

"Re your 145: New Enigma is intended for RED only."

The following day Berlin sent message No. 917 to the RED section, which read:

"INTERN 86. The new Enigma which arrived together with trunk transmitter is for RED. It is a birthday surprise for LUNA."

On the same day, 6 November, 1943, the RED section in Argentina sent message No. 991 requesting a Grund for the new Enigma, asking that it be sent via the BLUE key** and not via the RED Kryha key. This message went on to say that they were constantly making a fundamental blunder in transmitting a new key by means of the old one.

* Also solved independently by the British at about the same time.
** Unsolved.

TOP SECRET ULTRA

Berlin replied to this message on 9 November, 1945, asking the RED section to be patient for a few more days until a key for the new Enigma could be forwarded.

It was not, however, until 30 November, 1945, that Berlin sent messages Nos. 927, 928 and 929 which read:

"Exact set-up for the 'known machine' will follow as Nos. 951 to 947. These 27 messages will be enciphered as heretofore and thereafter super-enciphered with the 'known machine'. The Grundstellung required for this will be sent as No. 950 via BLUE. It is valid for these 27 messages only. (Your) message re Kryha understandable, although partly garbled after the word 'holes'. Therefore, after hole 9 we will open (hole) 12; 9-12 etc., beginning with message No. 948."

The latter portion of the above message was in reference to message No. 147 from Argentina which read:

"Due to Kryha defect, from messages Nos. 949 and 915, we will open the following holes: 2, 6, 9, 12, 13, 17, 21, 25, 26, 27, 29, 31, 33, 35, 39, 41, 43, 45, 47, 51. All other holes will be closed. Please advise from what number you will do likewise. We urgently require Grund for new Enigma."

It will be noted that Berlin stated that messages 951 to 947 were to be doubly enciphered and in the same message twice referred to "these 27 messages". If 27 messages were actually to be doubly enciphered, then the series would be Nos. 951 to 957. This seemed somewhat dubious since it appeared likely that all of the series were already enciphered and awaiting transmission and to assume that 27 messages were awaiting transmission could not be reconciled with the statement that the Kryha set-up would be changed beginning with message 948. On the other hand if the double-encipherment messages were not already enciphered it seemed logical to expect that the new Kryha setting would be used with message No. 951, the first of the series, since Berlin knew that the machine in Argentina was defective and presumably would not operate properly with the old sequence of holes open.

Moreover, it was probable that Berlin had missed completely the partly garbled portion after the word "holes" in Argentina's message No. 147 and that the new Berlin open hole sequence would possibly be 9, 12, 13, 17, etc., instead of 2, 6, 9, 12, etc. Consequently, if Berlin did encipher messages Nos. 931 to 947 as stated and then changed the Kryha setting at message No. 948 to encipher another 10 messages to make a total of 27, there were two possible Kryha settings which might be employed.

At any rate, message No. 930 was transmitted on 29 November, 1943, via the BLUE station, not in the BLUE key as requested but in the RED Kryha key. This message read:

"INTERN 100, Grundstellung: Wheel order II, III, I.
Ringstellung FFIR, Window setting DOXL. Start deciphering at once."

Messages 931 to 947 were transmitted on 30 November, 1943, 943 to 949 inclusive on 1 December, 1943, and 950 to 967 inclusive on 2 December, 1943.

On 30 November, 1943, Argentina transmitted message No. 913, in Kryha, saying:

"Your 931 and following numbers cannot be deciphered by Grundstellung in No. 930. Please check and transmit the right Grundstellung to us once more. Our wheels are numbered '0209'."

On 2 December, 1943, Argentina sent message No. 150, enciphered in the GREEN Enigma, which read:

"Your 931 to 949 cannot be deciphered in spite of INTERN 99 and 100. Check INTERN 100. We have machine 0209
....."

The above message then went on to repeat the numbers of open holes on the Argentina Kryha, and also requested that an explanation of Berlin's super-encipherment be sent via BLUE.

It will be noted that the above message indicates that Argentina expected the double-encipherment series would be composed of only 17 messages.

TOP SECRET ULTRA

Berlin, thinking that Argentina could not read the 931 series because of a misunderstanding on the Enigma Grund, sent message No. 963 on 3 December, 1943, which said:

"Following message, No. 964, was worked merely as a test, according to No. 961, without previous encipherment by Kryha. This is simply for your understanding."

According to message No. 962 of 3 December, 1943, message No. 961 was to be transmitted via BLUE. It was, but not until 7 days later when it was sent as No. 591 on 10 December, 1943, via BLUE.

Nothing further was heard from Argentina on whether they had read the 931 series and on 5 December, 1943, Berlin which meanwhile had evidently been doing some checking, sent messages Nos. 974 and 975, in which Berlin said:

"Re LUNA No. 13 and INTERN 104. We got the machines mixed up here, excuse it please. Nos 931 to 958 will be repeated. The first 16 messages immediately, the balance later because less important. Messages will have new lengths. These 16 messages follow as Nos. 976 to 996, i.e., 21 messages. First enciphered with Kryha, but with latest setting, then super-enciphered according to INTERN Nos. 100 and 104. Request immediate report whether it works this time. INTERN 108."

From this it appeared that Berlin and Argentina were finally about to get together and the typical confusion which existed up to this point would finally be clarified. There was no longer any doubt about the Kryha setting because by this time both sides of the circuit had their Kryha machines set to the "latest setting".

Berlin transmitted messages Nos. 978, 979 and 980 on 6 December, 1943, Nos. 976, 977 and 981 to 991 inclusive on 7 December, 1943, and messages Nos. 992 to 996 on 8 December, 1943.

On 8 December, 1943, Argentina sent message No. 915, in Kryha, saying: "It works! It works!"

On 11 December, 1943, Argentina stated in message No. 916, in Kryha, that the details for the 28th day of the month were missing but that otherwise all was clear.

TOP SECRET ULTRA

On 14 December, 1943, Berlin transmitted the following Kryha messages Nos. 906 and 907, a portion of which is quoted in the original German.

"We acknowledge receipt of 916 to 918. FEHLENDENDER J
ZWO A-T X TAG XX ROEM JXLJ KIN X DREI X ZWO JALJ LUDWIG
JULIUS OTTO CAESAR JXLJ GUSTAV WILLY OTTO ANTON JXLJ
KIN MUL HEUN ZWO JXLJ WUL PUMP AWT DREI XXX. Messages
963 to 973 with holes 13 and 24 open. Nos. 901 to 905
are enciphered with starting position stated in INTERN
No. 100.* Following message No. 908 is enciphered with
the 'known machine' in accordance with key set-up.
Until your confirmation whether deciphered we will
continue enciphering with Kryha. Holes 13 and 14
closed. Acknowledgment urgent. INTERN 112."

b. SOLUTION

When the series 931 to 947 and 948 to 957 inclusive were first received, work sheets were prepared in the manner described below, on which were indicated the 2 possible Kryha key sequences for the 948-957 series. These messages were also examined to determine whether messages could be superimposed. The results of this latter examination were favorable for some blocks of messages and quite poor for others. Moreover, no positive conclusion could be reached regarding whether the 948 to 957 series had had the same treatment as 931 to 947. The entire series did, however, reveal positive evidence of double encipherment in that nulls were added at the ends of messages with simple Enigma encipherment in such a way that it was evident that the text had originally consisted of 5-letter cipher groups which had been redivided into 4-letter groups.

Accordingly, in view of the uncertainties concerning the encipherment of the 931-947 and 948-957 series of messages, when it became known that the messages were being repeated, it was decided to attack the 976 to 996 series together with the 901 to 905 series known to have been enciphered by simple Enigma at the same Grund as the doubly enciphered messages.

* The Enigma starting position for the doubly enciphered messages.

TOP SECRET ULTRA

The commercial type of modified Kryha device which had been in use up to that time had the letters of the plain and cipher components arranged in the following sequences:

PLAIN: E S P F I T V O N A L D C H R B G J K M Q U W X Y Z

CIPHER: S V G D W M Q C J A H T E X R P N F I K U B Z L Y O

At the time these messages were enciphered, the following holes were open on the 52-hole control wheel: 2-6-8-12-13-17-23-24-27-29-31-35-39-41-43-45-47-51.

The basic starting point for all messages was with the plunger in hole No. 51 and the sequences juxtaposed so that B₀ was opposite P₀, and the machine then advanced from this basic position a number of steps equal to the last digit of the external message number. Thus, a message whose external number ended in the digits "1", "2", "5", etc., would be advanced 1, 2, or 5 places respectively from the basic starting point before the encipherment of the first letter. Messages whose number ended in 0 were advanced 10 places before the encipherment of the first letter. The alphabets generated from the above sequences can be arranged in a Vigenere square and labeled A to Z as shown in Figure 42.

SECRET ULTRA

E S P F I T V O N A L D C H R B G J K M Q U W X Y Z
 A S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 B O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 C Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 D L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 E Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 F B Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 G U B Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 H K U B Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 I I K U B Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 J F I K U B Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 K N F I K U B Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 L P N F I K U B Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 M R P N F I K U B Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 N X R P N F I K U B Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 O E X R P N F I K U B Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 P T E X R P N F I K U B Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 Q H T E X R P N F I K U B Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 R A H T E X R P N F I K U B Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 S J A H T E X R P N F I K U B Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 T C J A H T E X R P N F I K U B Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 U Q C J A H T E X R P N F I K U B Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 V M Q C J A H T E X R P N F I K U B Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 W W M Q C J A H T E X R P N F I K U B Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 X D W M Q C J A H T E X R P N F I K U B Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 Y G D W M Q C J A H T E X R P N F I K U B Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A
 Z V G D W M Q C J A H T E X R P N F I K U B Z L Y O S V G D W M Q C J A H T E X R P N F I K U B Z L Y O A

E S P F I T V O N A L D C H R B G J K M Q U W X Y Z

With the above details known, the sequence of alphabets used for the Kryha encipherment of a message will be found to be as follows:

1 2 3 4 5 6 7 8 9 0

Y I T W K K E H R Y G M T G N U C I V I V F Q T H U B E O V D J Q D

K R Z F S F S C N Q E R Y B L S A G N A H O W C P C P Z K N B O V Y

With this key sequence the key letters are found at the left hand margin of Figure 42, the cipher letters in the body of the square, and the plain letters at the top. The digits appearing over the

TOP SECRET ULTRA

First 10 letters of the key sequence indicate the starting cipher set for a message whose external number ends in "a", "aa", "aa", etc. Work sheets (Figure 43) were prepared containing the first 10 letters of messages 776 to 995 inclusive, (double encipherment) and Kryha alphabet key sequences written over the doubly enciphered messages. It will be noted that messages 10 apart start with the same key sequence, messages 10 apart have the key sequence slide 1 position to the left.

It is apparent that similar cipher letters in any given column of the work sheet must represent the same plain letter in messages 10 apart in number. Likewise, it is evident that similar cipher letters in any given column must decipher to the same Kryha cipher letter and that this first decipherment must be reciprocal. With these simple considerations in mind, let us examine repeated letters in a column. In column 1 the cipher letter "a" appears 5 times. Its appearances are in alphabets K, Y, W, T and in message 905 where it results from the encipherment of a plain letter by Enigma alone. Now, if we assume that the letter "a" deciphers to each of the Kryha cipher component letters in turn (excluding S), we can, since we know the Kryha alphabets, state that the plain text must consist of the letters contained in some column from the following table:

Assumed 1st Decipherment

			S	V	G	D	W	M	Q	C	J	A	H	T	E	X	R	P	N	F	I	K	U	B	Z	L	Y	O
Required	SR	J	K	M	Q	U	W	X	Y	Z	E	S	P	F	I	T	V	O	N	A	L	D	C	H	R	B	O	
Plain	SY	Y	Z	E	S	P	F	I	T	V	O	N	A	L	D	C	H	R	B	F	J	K	M	Q	U	N	A	
	SW	W	X	Y	Z	E	S	P	F	I	T	V	O	N	A	L	D	C	H	R	B	O	J	K	M	Q	U	
	ST	M	Q	U	W	X	Y	Z	E	S	P	F	I	T	V	O	N	A	L	D	C	H	R	B	O	J	K	
	Se	S	V	G	D	W	M	Q	C	J	A	H	T	E	X	R	P	N	F	I	K	U	B	Z	L	Y	O	

In the above table, the final S comes from a single Enigma encipherment, therefore, the successive possible plain values are shown with the Kryha cipher component, the doubly enciphered letters have been converted to their Kryha plain component equivalents.

In addition to the above type of tables for repeated letters in columns it was found convenient to weight each column of possible plain letters by the product of the frequencies of the individual

TOP SECRET ULTRA

letters contained in each column of the table. This was accomplished by assigning the following natural log weights to the individual letters.

E	7.2	S	6.4
S	6.4	V	4.6
P	4.9	G	5.5
F	5.4	D	5.6
I	6.5	W	5.1
T	6.4	M	5.1
V	4.6	Q	5.0
O	6.2	C	5.5
N	6.8	J	6.4
A	6.4	A	6.4
L	6.0	V	5.3
D	5.6	T	6.4
C	5.5	E	7.2
H	5.3	X	6.0
R	6.5	R	6.5
B	5.1	P	4.9
G	5.5	N	6.8
J	6.4	F	5.4
K	5.1	I	6.5
M	5.1	K	5.1
Q	5.0	U	6.0
U	6.0	B	5.1
W	5.1	Z	4.8
X	6.0	L	6.0
Y	4.5	Y	4.5
Z	4.8	O	6.2

Master cards for IBM tabulating machines were prepared with these sequences of weights and the appropriate values ganged into the cipher text cards. The cards were then sorted into blocks of similar cipher letters in the same columnar position on the work sheet and the log weights were added into 26 5-digit counters on the tabulator, with the controls so set that the counters cleared and printed a total after the passage of each block.

TOP SECRET ULTRA

Consider the following from columns 34 and 40 of the work sheet.

	S	V	G	D	W	M	Q	C	J	A	H	<u>COLUMN 34</u> Y	X	R	P	N	P	I	K	V	B	Z	L	Y	0
C	P	F	I	T	V	O	N	A	L	D	C	H	R	B	Q	J	K	M	Q	U	W	X	Y	Z	8
F	T	K	O	M	A	L	I	C	H	E	S	G	F	K	M	Q	U	W	X	Y	Z	8	9	9	9
R	J	V	Q	U	W	X	I	T	Z	E	S	P	F	I	T	V	O	N	A	L	D	C	H	E	9
O	K	M	Q	U	W	X	I	T	Z	E	S	P	F	I	T	V	O	N	A	L	D	C	H	E	9
Z	E	S	P	F	I	T	V	O	N	A	L	D	C	H	E	S	P	F	I	T	V	O	N	A	9
Weights	324	346	356	340	329	363	355	300	357	393	345	331	360	337	322	352	343	344	362	321	310	338	345	352	334

	S	V	G	D	W	M	Q	C	J	A	H	<u>COLUMN 40</u> Y	X	R	P	N	P	I	K	V	B	Z	L	Y	0
A	S	V	G	D	W	M	Q	C	J	A	H	T	E	X	R	P	N	P	I	K	V	B	Z	L	Y
F	T	K	O	M	A	L	I	C	H	E	S	G	F	K	M	Q	U	W	X	Y	Z	8	9	9	9
Weights	192	138	172	180	166	162	156	159	181	193	157	183	208	117	181	148	196	159	190	145	168	174	160	169	140

Considering both the weights and the identities of the plain text letters involved it appears that an A/O Enigma reciprocal pair in column 34 is an excellent assumption.

	S	V	G	D	W	M	Q	C	J	A	H	<u>COLUMN 40</u> Y	X	R	P	N	P	I	K	V	B	Z	L	Y	0
J	S	V	G	D	W	M	Q	C	J	A	H	T	E	X	R	P	N	P	I	K	V	B	Z	L	Y
C	P	F	I	T	V	O	N	A	L	D	C	H	R	B	Q	J	K	M	Q	U	W	X	Y	Z	8
L	P	F	I	T	V	O	N	A	L	D	C	H	R	B	Q	J	K	M	Q	U	W	X	Y	Z	8
Y	P	F	I	T	V	O	N	A	L	D	C	H	R	B	Q	J	K	M	Q	U	W	X	Y	Z	8
Weights	313	318	344	276	316	341	371	339	325	335	359	334	372	317	320	361	362	344	329	365	333	308	337	343	360

TOP SECRET ULTRA

With the values resulting from the A/O Enigma pair in column 54 entered on the work sheet the high weight values were tried in turn in column 40 until the J/L Enigma pair was tested. With these values added to those already entered in column 54, a "Z" appeared in column 40 of message No. 995. This was tentatively assumed to be the beginning of "ZWO". Progressive steps in the deciphering of the messages are shown in Work Sheets 1 to 10.

TOP SECRET ULTRA

WORK SHEET NO. 1

	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	
976	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H	
	T	M	E	T	O	N	U	G	P	W	J	V	W	D	N	R	Y	L	B	V		
					A						L	A										
977	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H	O	
	E	L	Q	I	T	V	M	Z	Y	F	B	W	L	B	D	Q	C	E	L	Y	N	
978	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H	O	W	
	S	H	C	H	I	Z	Q	F	V	D	M	Q	B	I	O	Q	L	C	L	W	S	
979	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H	O	W	C	
	Y	N	D	W	M	M	Y	R	P	S	X	B	I	Z	Y	T	W	X	Z	S	J	
980	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H	O	W	C	P	
	W	T	S	O	J	Y	R	F	S	J	J	U	Q	G	B	I	R	C	C	A	D	
981	V	D	J	Q	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	
	W	K	V	O	Q	T	U	K	X	I	O	Q	U	V	Y	J	S	F	O	U	Y	
982	D	J	Q	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	
	H	P	A	H	C	F	T	O	X	K	S	D	O	H	M	C	M	M	Z	B	I	
983	J	Q	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	
	H	S	Z	V	R	H	B	Z	D	X	T	H	K	Z	N	G	S	Q	T	H	K	
984	Q	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	
	K	B	O	D	Z	X	V	H	M	H	M	N	U	L	O	P	R	K	Z	A		
					A																	
985	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	
	Y	B	O	V	S	B	K	G	T	X	C	Q	U	V	P	B	R	C	Y	I		
986	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H	
	T	C	Y	Z	B	I	D	W	I	V	N	X	M	Y	N	N	H					

TOP SECRET ULTRA

WORK SHEET NO. 1 (CONT'D)

50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70

987 R Z F S F S C N Q E R Y B L S A G N A H O
H T C L P G X T X F K S I R I I D R A D X

988 Z F S F S C N Q E R Y B L S A G N A H O W
L O F U F V G T R A J E F E K U U T W L M
L T
u w

989 F S F S C N Q E R Y B L S A G N A H O W C
F W Q I O K S R V P E W C C S Z G W X I R
A
d

990 S F S C N Q E R Y B L S A G N A H C W C P
A R W E Y P R W D O J N O E A H A R O I H
L
n

991 V D J Q D K R Z F S F S C N Q E R T B L S
I L P X U W F W D C I H S U R J R T Z I W

992 D J Q D K R Z F S F S C N Q E R Y B L S A
X W T V D T G S T I Q S D M O Q L S R N K

993 J Q D K R Z F S F S C N Q E R Y B L S A G
G L E J O K U I A D J V T A I U E I U Z J
A
e L A F
s w o

994 Q D K R Z F S F S C N Q E R Y B L S A G N
X M Q T O T A M L I C Y D C D W Z C Z V T
A
n

995 D K R Z F S F S C N Q E R T B L S A G N A
Y Y N C O D W L L G G A Z N T M L N F G C
A
r v
t

996 K R Z F S F S C N Q E R Y B L S A G N A H
B O M P G B J P O W W Z A U N H J J D Y R

TOP SECRET ULTRA

WORK SHEET NO. 1 (CONT'D)

	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	00
901	A	D	S	A	A	U	D	B	U	I	U	V	F	Q	I	T	P	S	A	H	
902	O	O	W	F	R	L	E	R	Q	U	X	S	Q	J	D	S	Q	D	O	B	
903	E	H	F	K	W	X	E	A	Y	E	X	J	V	Q	R	D	U	N	D	H	O
904	A	C	V	O	Y	E	N	N	J	W	J	W	S	J	V	X	J	P	L	L	S
											1										
905	E	B	O	W	A	I	O	R	E	J	K	D	I	F	E	D	V	W	P	S	E

Assumptions:

A equals O, and O equals A in col. 84

J equals L, and L equals J in col. 40

Message 993, col. 40, reads "ZWO"

TOP SECRET ULTRA

WORK SHEET NO. 2

30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

976 K R Z F S F S C N Q E R Y B L S A G N A H
T M E T O N U G P W J V V W D W R Y L B V
A
s

977 R Z F S F S C N Q E R Y B L S A G N A H O
E L Q I T V M Z Y F B W L B D Q C E L Y N

978 Z F S F S C N Q E R Y B L S A G N A H O W
S H C H I Z Q F V D M Q B I O Q L C L W S

979 F S F S C N Q E R Y B L S A G N A H O W C
Y N D W M M Y R P S X B I Z Y T W X Z S J

980 S F S C N Q E R Y B L S A G N A H O W C P
W T S O J Y R F S J J U Q G B I R C C A D
L
n

981 V D J Q D K R Z F S F S C N Q E R Y B L S
W K V O Q T U K X I O Q U V Y J S F O U Y

982 D J Q D K R Z F S F S C N Q E R Y B L S A
H P A H C F T O X K S D O H M C M M Z B I
A
r

983 J Q D K R Z F S F S C N Q E R Y B L S A G
H S Z V R H B Z D X T H K Z N G S Q T H K
E
s
l

984 Q J K R Z F S F S C N Q E R Y B L S A G N
K B G D O Z X V H M H M N U L O P R K Z A
A
n

985 D K R Z F S F S C N Q E R Y B L S A G N A
Y B O V A S B K G T X C J U V P B R C Y I
O
i

TOP SECRET ULTRA

WORK SHEET NO. 2 (CONT'D)

	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
986	K T	R C	Z Y	F Z	S B	F I	S D	C W	N I	Q V	R N	R X	Y M	B Y	L N	S N	A H	A A	Q Q	V V	H H
987	R H	Z T	F C	S L	F P	S G	C X	N T	Q I	E F	R K	Y S	B I	L R	S I	A I	Q D	H A	H D	O E	
988	Z L	F O	S F	F U	S T	C V	N G	Q T	E R	R A	Y J	B E	L F	S F	A K	Q U	N U	H S	O L	W M	
989	F F	S W	F Q	S I	C O	N K	Q S	E R	R V	Y P	B E	L W	S C	A C	Q S	N Z	A J	H X	O I	W C	
990	S A	F R	S W	C E	N Y	Q P	E R	R W	Y D	B O	L J	S N	A O	G E	N A	H A	H A	O R	O I	F H	
991	V I	D L	J P	Q X	D W	K F	R W	Z F	S D	F C	S H	C S	N U	Q R	E J	R R	Y T	B Z	L I	S W	
992	D X	J W	Q T	D V	K D	R T	Z G	F S	S T	F I	S Q	C S	N D	Q M	E O	R Q	Y L	B S	L R	S N	
993	J J	Q L	D E	K J	R O	Z K	F U	S I	F A	S D	C J	N V	Q A	E I	R Y	Y U	B E	L I	S U	A Z	
994	J X	D M	K Q	R T	Z O	F R	S A	F M	S L	C I	N C	Q Y	E D	R C	Y D	B C	L D	S W	A Z	N T	

TOP SECRET ULTRA

WORK SHEET NO. 3

	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
976	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H
	T	M	E	T	O	H	U	G	P	W	J	V	V	W	D	N	R	Y	L	B	V
					A						L	A	K								
					S						S	•	J								
977	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H	O
	E	L	Q	I	T	V	M	Z	Y	F	B	W	L	B	D	Q	C	E	L	Y	N
								T								Q					
								Y								P					
978	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H	O	W
	S	H	C	H	I	Z	Q	F	V	D	M	Q	B	I	O	Q	L	C	L	W	S
																Q					
																n					
979	F	B	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H	O	W	C
	Y	N	D	W	M	M	Y	R	P	S	X	B	I	Z	Y	T	N	X	Z	S	J
															F						
															J						
980	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H	O	W	C	P
	W	T	S	O	J	Y	R	F	S	J	J	U	Q	G	B	I	R	C	C	A	D
											L										
											n										
981	V	D	J	Q	D	K	R	Z	F	S	F	S	C	V	Q	E	R	Y	B	L	S
	W	K	V	O	Q	T	U	K	X	I	O	Q	U	V	Y	J	S	F	O	U	Y
																U					
																d					
982	D	J	Q	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A
	H	P	A	H	C	F	T	O	X	K	S	D	O	H	M	C	M	M	Z	B	I
										A											
										r											
983	J	Q	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G
	H	S	Z	V	H	H	B	Z	D	X	T	H	K	Z	N	G	S	Q	T	H	A
								T	A	E	D	E	V	F	K	Q	U	N			
								f	r	i	t	s	j	u	l	i	u	s			

TOP SECRET ULTRA

WORK SHEET NO. 3 (CONT'D)

30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

984 Q D K R Z F S F S C N Q E R Y B L S A G N
K B G D O Z I V H M H M N U L O P R K Z A
A
n

985 D K R Z F S F S C N Q E R Y B L S A G N A
Y B O V A S 9 K G T X C Q U V P B R C Y I
O
i

986 K R Z F S F S C N Q E R Y B L S A G N A H
T C Y Z B I D W I V N X M Y N N H A Q V Q
K
i

987 R Z F S F S C N Q E R Y B L S A G N A H O
H T C L P G X T X F K S I R I I D R A D X
Z
a

988 Z F S F S C N Q E R Y B L S A G N A H O W
L O F U T V G T R A J E F F K U U T W L M
Z
c l u d w i g

989 F S F S C N Q E R Y B L S A G N A H O W C
F W Q I O K S R V P E W C C S Z G W X I R

990 S F S C N Q E R Y B L S A G N A H O W C P
A R W E Y P R W D O J N O E A H A R O I H
A
o n x

991 V D J Q D K R Z F S F S C N Q E R Y B L S
I L P X U W F W D C I H S U R J R T Z I W
A
r i

992 D J Q D K R Z F S F S C N Q E R Y B L S A
X W T V D T G S T I Q S D M O Q L S R N K
G
m

WORK SHEET NO. 3 (CONT'D)

30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

993 J Q D K R Z F S F S C N Q E R Y B L S A G
 J L E J O K U I A D J V T A I U E I U Z J
 A e n s w o

994 Q D K R Z F S F S C N Q E R Y B L S A G H
 X M Q T O R A M L I C Y D C D W Z C Z V T
 A n

995 D K R Z F S F S C N Q E R Y B L S A G H A
 Y Y N C O D W L L G G A Z N T M L N F G C
 A r v v

996 K R Z F S F S C N Q E R Y B L S A G H A H
 B O M P G B J P O W W Z A U N H J J D Y R
 K 1

901 A D S A A U D B O I U Y V P Q I T P S A H
 o k

902 O O W F R L Z E C Q U X S Q J D S Q D G B
 u n

903 Z H F K W X Z A Y Z X J V Q R D U H D H G
 k q

904 A C V O Y Z N N J W J W S J V X J P L L S
 1

905 E B O W A I O R Z J K D I F E D V N P S E
 o q
 (Z) CONTRADICTION

Assumption:

FRITZJULIUS 983 Col. 37 (Rejected)

TOP SECRET ULTRA

WORK SHEET NO. 4

30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

976 K R Z F S F S C N Q E R Y B L S A G N A H
T M E T O N U G P W J V V W D N R Y L B V
A
s

977 R Z F S F S C N Q E R Y B L S A G N A H O
E L Q I T V M Z Y F B W L O
o

978 Z F S F S C N Q E R Y B L S A G N A H O W
S H C H I Z Q F V D M Q B I O Q L C L W S

979 F S F S C N Q E R Y B L S A G N A H O W C
Y N D W M M Y R P S X B I Z Y T W X Z S J

980 S F S C N Q E R Y B L S A G N A H O W C P
W T S O J Y R F S J J U Q Q B I R C C A D
L
n

981 V D J Q D K R Z F S F S C N Q E R Y B L S
W K V O Q T U K X I O Q U V Y J S F O U Y

982 D J Q D K R Z F S F S C N Q E R Y B L S A
H P A H C F T O X K S D O H M C M M Z B I
A
F
L
1

983 J Q D K R Z F S F S C N Q E R Y B L S A G
H S Z V R H B Z D X T H K Z N G S Q T H K
E
s
K
1

984 Q D K R Z F S F S C N Q E R Y B L S A G N
K B G D O Z X V H M H M N U L O P R K Z A
A
n

985 D K R Z F S F S C N Q E R Y B L S A G N A
Y B O A S S K G T X C Q U V P B R C Y I
O
1

TOP SECRET ULTRA

WORK SHEET NO. 4 (CONT'D)

30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

986 R R R F S F S O N Q R R I B L S A G M A H
T O Y A D I D W I V N X M Y K N N H A Q V Q
K
1

987 R R F R F S G N Q R R Y B L S A G M A H O
H T O L P O X T X F K S I R I I D R A D X

988 R F R F S O N Q R R Y B L S A G M A H O W
L O F U T V G T R A K J R F ' K U U T W L M
K L H T E N
I u d w i e

989 F S F S O N Q R R Y B L S A G M A H O W C
F W Q I O N S R V F E W O C S Z G W X I R
A
d

990 B F S O N Q R R Y B L S A G M A H O W C P
A R W E Y P R W D O J N O L F W A H A R O I H
L O L F W
B J X X J

991 V D J Q D K R Z F S F S O N Q R R Y B L S
I L P X U W F W D O I H S U R J R T Z I W
E
1

992 D J Q D K R Z F S F S G N Q R R Y B L S A
X W T V D T U U T I Q S D M O J L S R N K

993 J Q D K R Z F S F S G N Q R R Y B L S A G
O L E J O K U I A D J V T A I U S I U Z J
A
e
S W O

994 Q O K R Z F S F S G N Q R R Y B L S A G N
X M Q T O R A M L I C Y D C D W Z C Z V T
A
n

TOP SECRET ULTRA

WORK SHEET NO. 4 (CONT'D)

	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
995	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A
	Y	Y	N	C	O	D	W	L	L	G	G	A	Z	N	T	M	L	N	F	G	C
					A							V									
					r							t									
996	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H
	B	O	M	P	O	B	J	P	O	W	W	Z	A	U	N	H	J	J	D	Y	R
															K						
															1						
901	A	D	S	A	A	U	D	B	G	I	U	Y	V	P	Q	I	T	P	S	A	H
					O																
902	O	O	W	F	R	L	Z	E	C	Q	U	X	S	Q	J	D	S	Q	D	3	B
903	Z	H	F	K	W	X	Z	A	Y	Z	X	J	V	Q	R	D	U	N	D	H	G
904	A	C	V	O	Y	Z	N	N	J	W	J	W	S	J	V	X	J	P	L	L	S
											1										
905	E	B	O	W	A	I	O	R	Z	J	K	D	I	F	E	D	V	N	P	S	E

Assumptions:

IX 990/42

JXXJ 990/41

TOP SECRET ULTRA

WORK SHEET NO. 5

30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

976 K R Z F S F S C N Q E R Y B L S A G N A H
T M E T O N U G P W J V V W D N R Y L B V
A S L A S

977 R Z F S F S C N Q E R Y B L S A G N A H O
E L Q I T V M Z Y F B W L O B D Q C E L Y N
O

978 Z F S F S C N Q E R Y B L S A G N A H O W
S H C H I Z Q F V D M Q B I O Q L C L W S

979 F S F S C N Q E R Y B L S A G N A H O W C
Y N D W M M Y R P S X B I Z Y T W X Z S J
V S

980 S F S C N Q E R Y B L S A G N A H O W C P
W T S O J Y R F S J J U Q G B I R C C A D
L n

981 V D J Q D K R Z F S F S C N Q E R Y B L S
W K V O Q T U K X I O Q U V Y J S F O U Y
Z H r s

982 D J Q D K R Z F S F S C N Q E R Y B L S A
H P A H C F T O X K S D O L M C M M Z B I
A r l

983 J Q D K R Z F S F S C N Q E R Y B L S A G
H S Z V R H B Z D X T H K Z N G S Q T H K
E H V K L H T E N
z e t l u d w i g

984 J D A R Z F S F S C N Q E R Y B L S A G N
A B G D O Z X V H M H M N U L O R L G A
A n

TOP SECRET ULTRA

WORK SHEET NO. 5 (CONT'D)

	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
985	D Y	K B	R O	Z V	F A O 1	S S	F B	S K	C G	N T	Q X	E R	Y C	B Q	L U	V P	S B	A R	G C	N Y	I I
986	K T	R C	Z Y	F Z	S B	F I	S D	C W	N I	Q V	E R	X N	Y M	B Y	L N K 1	S N	A H S e	G A	N Q	A V	H Q
987	R H	Z T	F C	S L	F P	S G	C X	N T	Q X	E F	R K	Y S	B I	L R	S I	A I	J D	N R	A H	O X	
988	Z L	F O	S F	F U	S T	C V	N G	Q T	E R	Y A K L	B J E H d	L F T w	S F F e	A K N g	G U	N U	A T q v	H O w l m			
989	F F	S W	F Q	S I	C O A d	N K	Q S	E R	V P	Y B	E W	L S	A C	G S	N Z	A G	H O	X I	R C		
990	S A	F R	S W	C E	N Y	Q P	E R	Y W	B D	L J L n	S N O J	A O L x	G E W j	N A H	H A	H O	W R	C O	P I		
991	V I	D L	J P	Q X	D U	K W	R F	Z W	F D	S C	F I	S H E 1	C S	N U	Q R	E J	R Y	T Q 1	B Z	L I	S W
992	D X	J W	Q T	D V	K D	R T	Z G	F S	T I	S Q	C S	N D	Q M	E O	R Q	Y L	B S	R H	S P	N A	
993	J G	Q L	D E	K J	R O	Z K	F U	S I	A D	S J	C V	N L	Q A	E T	R I	Y U	B E	L I	S C	A Z	G J

TOP SECRET ULTRA

WORK SHEET NO. 5 (CONT'D)

	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
994	Q	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N
	X	W	Q	T	O	R	A	M	L	I	C	Y	D	C	D	W	Z	C	Z	V	T
					A																
995	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A
	i	Y	N	C	O	D	W	L	L	G	G	A	Z	N	T	M	L	N	F	O	C
					A							V									
					r							t									
996	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H
	B	O	M	P	G	B	J	P	O	W	W	Z	A	U	N	H	J	J	D	Y	R
															K						
															i						
901	A	D	S	A	A	U	D	B	G	I	U	Y	V	P	Q	I	T	P	S	A	H
					O																
902	O	O	W	F	R	L	Z	E	C	Q	U	X	S	Q	J	D	S	Q	D	G	B
																	h	t			
903	Z	H	F	K	W	X	Z	A	Y	Z	X	J	V	Q	R	D	U	N	D	H	G
																			n		
904	A	C	V	O	Y	Z	N	N	J	W	J	W	S	J	V	X	J	P	L	L	S
											l										
905	E	B	O	W	A	I	O	R	Z	J	K	D	I	F	E	D	V	N	P	S	E

Assumptions:

ZETLUDWIG 983/41

TOP SECRET ULTRA

WORK SHEET NO. 6

30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

976 K R Z F S F S C N Q E R Y B L S A G N A H
T M E T O N P I K X T L A E
s q l u e s s e l

977 R Z F S F S C N Q E R Y B L S A G N A H O
E L Q I T V M Z Y F B W L O
e

978 Z F S F S C N Q E R Y B L S A G N A H O W
S H C H I Z Q F V D M Q B I O Q L C L W S

979 F S F S C N Q E R Y B L S A G N A H O W C
Y N D W M M Y R P S X B I A Z V
i s m

980 S F S C N Q E R Y B L S A G N A H O W C P
W T S O J Y R F S J L U Q G B I R C C A D
L n

981 V D J Q D K R Z F S F S C N Q E R Y B L S
W K V O Q T U K X I O Q U V Y J S F O U Y
I P z
a q s

982 D J Q D K R Z F S F S C N Q E R Y B L S A
H P A H C F T O X K S D O H M C M M Z B I
P A L
o r l

983 J Q D K R Z F S F S C N Q E R Y B L S A G
H S Z V R H B Z D X T H K Z N G S J T H K
E H V K L H T E N
z e t l u d w i s

984 J D K R Z F S F S C N Q E R Y B L S A G N
K B C D O Z X V H M H M N U L O P R K Z A
A
n i

TOP SECRET ULTRA

WORK SHEET NO. 6 (CONT'D)

30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

985 D K R Z F S F S C N Q E H Y B L S A I N A
Y B O V A S B K G T X C Q U V P B R C Y I
O
i
q
j

986 K R Z F S F S C N Q E R Y B L S A G N A H
T C Y Z B I D W I V N X M Y L N N S A Q V Q
K
i
e

987 R Z F S F S C N Q E R Y B L S A G N A H O
H T C L P G X T X F K S I R I I D R A D X
P
t

988 Z F S F S C N Q E R Y B L S A G N A H O W
L O F U T V J T R A J E F F K U U T W L M
K L U T S N F Z Q K S
l u d w i e x a v e r

989 F S F S C N Q E R Y B L S A G N A H O W C
F W Q I O K S R V P E W C C S Z G W X I R
A
d

990 S F S C N Q E R Y B L S A G N A H O W C P
A R W E Y P R W D O J N O E A H A R O I H
N
v
L O L F W
n j x x j

991 V D J Q D K R Z F S F S C I Q E R Y B L S
I L P X U W F W D C I H S U R J R T Z I W
E
i
Q
i

992 D J Q D K R Z F S F S C N Q E R Y B L S A
X W T V D T G S T I Q S D M O Q L S R N K
H
P

TOP SECRET ULTRA

WORK SHEET NO. 6 (CONT'D)

30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

993 J Q D K R Z F S F S C N Q E R Y B L S A G
G L E J O K H I A D J V T A I J F
x z w o b

994 Q D K R Z F S F S C N Q E R Y B L S A G N
X M Q T O R A M L T C Y D C L W Z U
n t

995 D K R Z F S F S C N Q E R Y B L S A G N A
Y Y N C O D W L L G G A V
r t

996 K R Z F S F S C N Q E R Y B L S A G N A
B O M P G B J P O W W Z A U N H J J D Y R
T K
s i

901 A D S A A U D B G I U Y V P Q I T P S A H
o e

902 O O W F R L Z E C Q U X S Q J D S Q D G B
n t

903 Z H F K W X Z A Y Z X J V Q R D U N D H G
e z n

904 A C V O Y Z N N J W J W S J V X J P L L S
t l s

905 E B O W A I O R Z J K D I F E D V N P S E
e l

Assumptions:

XAVER 988/39

SQUESSEL 976/34

TOP SECRET ULTRA

WORK SHEET NO. 7

30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

976 K R Z F S F S C N Q E R Y B L S A J K A H
T M E T J N U G P W J L A E I
s q l u e s s e l

977 R Z F S F S C N Q E R Y B L S A G N A H O
E L Q I T V M Z Y F B W L O
e

978 Z F S F S C N Q E R Y B L S A G N A H O W
S H C H I Z Q F V D M J B I O Q L C L W S
e a

979 F S F S C N Q E R Y B L S A G N A H O W C
Y N D W M M Y R P S X B I Z Y T W X Z S J
X i v s m

980 S F S C N Q E R Y B L S A G N A H O W C P
W T S O J Y R F S J J U Q G B I R C C A D
S i n

981 V D J Q D K R Z F S F S C N Q E R Y B L S
W K V O Q T U K X I O Q U V Y J S F O U Y
U I G P E D J Z H
m a s q i n e r s

982 D J Q D K R Z F S F S C N Q E R Y B L S A
H P A H C F T O X K S D O H M C M M Z B I
P A L
o r l

983 J Q D K R Z F S F S C N Q E R Y B L S A G
H S Z V R H B Z D X T H K Z N G S Q T H K
G e t l u d w i g
o z e t l u d w i g

WORK SHEET NO. 7 (CONT'D)

292

TOP SECRET ULTRA

WORK SHEET NO. 7 (CONT'D)

	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
992	D	J	Q	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A
	X	W	T	V	D	T	G	S	T	I	Q	S	D	M	O	Q	L	S	R	N	K
					U					E										H	
					d					J										P	
995	J	Q	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G
	G	L	E	J	O	K	U	I	A	D	J	V	T	A	I	U	E	I	U	Z	J
						I				O	L	A	F								
						x				J	z	w	o			b					
994	Q	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N
	X	M	Q	T	A	R	A	M	L	I	C	Y	D	C	D	W	Z	C	Z	V	T
					n					r						U					
																t					
995	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A
	Y	Y	N	C	O	D	W	L	G	G	A	Z	N	T	M	L	N	F	G	C	
					A			W				V									
					r			w				t									
996	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H
	B	O	M	P	G	B	J	P	O	W	W	Z	A	U	N	H	J	J	D	Y	R
										T											
										s						K					
																i					
901	A	D	S	A	A	U	D	B	G	I	U	Y	V	P	Q	I	T	P	S	A	H
				o		t			d	e			e								
902	O	O	W	F	R	L	Z	E	C	Q	U	X	S	Q	J	D	S	Q	D	G	B
																		h	t		
903	Z	H	F	K	W	X	Z	A	Y	Z	X	J	V	Q	R	D	U	N	D	H	G
												q	e				z		n		
904	A	C	V	O	Y	Z	N	N	J	W	J	W	S	J	V	X	J	P	L	L	S
									t	l									r	s	
905	E	B	O	W	A	I	O	R	Z	J	K	D	I	F	E	D	V	N	P	S	E
													e								l

Assumptions:

MASQINE 981/35
 DORA 982/37 (Rejected)
 VIREIN 990/35

TOP SECRET ULTRA

WORK SHEET NO. 9

30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

976 L R Z F S F S C N Q E R Y B L S A G N A H
T M E T O N U G P W J V V W D N R Y L B V
A P I K X T L A E
s q l u e s s e l

977 R A F S F S C N Q E R Y B L S A G N A H O
E L Q I T V M Z Y F B W B L S A G N A H O
L O
e

978 Z F S F S C M Q E R Y B L S A G N A H O W
S H C H I Z Q F V D M Q B B I O Q L C L W S
S
P O J a

979 F S F S C N Q E R Y B L S A G N A H O W C
Y N D W M M Y R P S X B I Z Y T W X Z S J
X V L
i s m

980 S F S C N Q E R Y B L S A G N A H O W C P
W T S O J Y R F S J J U Q G B I R C C A D
S L
i n

981 V D J Q D K R Z F S F S C N Q E R Y B L S
W K V O Q T U K X I O Q U V Y J S F O U Y
U I G P E D J Z H
m a s s q i n e r s

982 D J Q D K R Z F S F S C N Q E R Y B L S A
H P A H C P T O X K S D O H M C M M Z B I
P A L
o r

983 J Q D K R Z F S F S C N Q E R Y B L S A G
H S Z V R H B Z D X T N H K Z N G S Q T H K
C W G E H V K L H T E N
J a o z e t l u d w i g

TOP SECRET ULTRA

WORK SHEET NO. 11 (CONT'D)

	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	
984	C	D	K	R	E	F	S	F	S	C	N	Q	K	R	Y	B	L	S	A	G	H
	K	B	O	D	A	S	X	V	N	M	N	M	N	U	L	O	P	R	K	Z	A
					n	t															
985	D	K	R	E	F	S	F	S	C	N	Q	K	R	Y	B	L	S	A	G	N	A
	Y	R	O	V	A	S	B	K	O	T	X	C	Q	U	V	P	R	C	Y	I	
				C	W	Q	D	W	J												
				v	i	r	a	q	t	j											
986	K	R	E	F	S	F	S	C	N	Q	K	R	Y	B	L	S	A	G	N	A	H
	T	C	Y	Z	B	I	D	W	I	V	N	X	M	Y	N	N	H	A	Q	V	Q
							L	A							K	S					
							s	w							1	e					
987	R	Z	F	S	F	S	C	N	Q	K	R	Y	B	L	S	A	G	N	A	H	O
	H	T	C	L	P	O	X	T	X	F	K	S	I	R	I	I	D	R	A	D	X
									P	t											
988	Z	F	S	F	S	C	N	Q	K	R	Y	B	L	S	A	G	N	A	H	O	W
	L	O	F	U	T	V	G	T	R	A	J	E	F	F	K	U	U	T	W	L	M
									K	L	H	T	E	N	F	Z	Q	K	S		
									l	u	d	w	i	e	x	a	v	e	r		
989	F	S	F	S	C	N	Q	K	R	Y	B	L	S	A	G	N	A	H	O	W	C
	F	W	Q	I	O	K	S	R	V	P	E	W	C	C	S	Z	O	W	X	I	R
				A			R														
				d			1														
990	S	F	S	C	N	Q	K	R	Y	B	L	S	A	G	N	A	H	O	W	C	P
	A	R	W	E	Y	P	R	W	D	O	J	N	O	E	A	H	A	R	O	I	H
					N	S	L	O	D	L	O	L	F	W							
					v	i	r	e	i	n	j	x	x	j							
991	V	D	J	Q	D	K	R	Z	F	S	F	S	C	N	Q	K	R	Y	B	L	S
	I	L	P	X	U	W	F	W	D	C	I	H	S	U	R	J	R	T	Z	I	W
						J	L	G			E										
						s	w	o			1										
																				1	

TOP SECRET ULTRA

WORK SHEET NO. 8 (CONT'D)

50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70

992 D J Q D K R Z F S F S C N Q E R Y B L S A
X W T V D T G S T I Q S D M O Q L S R N H K
C l u d j p

995 J Q D K R Z F S F S C N Q E R Y B L S A G
G L E J O K U I A D J V T A I U E I U Z J
I M I O L A F f
x x x j z w o b

994 Q D K R Z F S F S C N Q E R Y B L S A G N
X M Q T O R A M L I C Y D C W L Z C A Z V T
n i e r u t

995 D K R Z F S F S C N Q E R Y B L S A G N A
Y I N C O D W L L G G A Z N T M L N F G C
V A B W v t
e r e w

996 K R Z F S F S C N Q E R Y B L S A G N A H
B O M P G B J P O W W Z A U N H J J D Y R
F T K i
a s

901 A D S A A U D B G I U Y V P Q I T P S A H
o t d e e

902 O O W F R L Z E C Q U X S Q J D S Q D G B
h t

903 Z H F K W X Z A Y Z X J V Q R D U N D H G
q e s n

904 A C V O Y Z N N J W J W S J V X J P L L S
s t l s

905 E B O W A I O R Z J K D I F E D V N P S E
e l

Assumptions:

VIRAQT 985/33

ZWO 991/36

XX 995/37

001 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20

077 H H F H F H G H Q H H Y H L B A O H A H O
H H L Q I T V M N Y T F V B W L O N D Q C E L Y N

979 F B F B O N Q K R Y B L S A O N A H O W C
Y N D W M M Y R P X B I Z Y T W X Z S J
X
d
v
e

	V	D	J	Q	D	K	R	Z	F	S	P	S	C	N	Q	E	R	Y	B	L	S
901	W	K	V	O	Q	T	U	X	I	O	D	J	U	V	X	J	S	F	O	U	Y
						U	a	s	e	i	n	e		r			H				

905 J Q D K R Z F S F S C N Q E R Y B L S A G
H S Z V R H B S D X T H K Z N O S Q T H N K
C
1 a o i s e t l u d w i g

TOP SECRET ULTRA

WORK SHEET NO. 9 (CONT'D)

	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70
984	Q	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N
	K	B	G	D	O	Z	X	V	H	M	H	M	N	U	L	O	P	R	K	Z	A
					A	S													W		
					n	t													i		
985	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A
	Y	B	O	V	A	S	B	K	G	T	X	C	Q	U	V	P	B	R	C	Y	I
				C	O	Z	W	G	D	W											
				v	i	r	a	q	t	j											
986	K	R	Z	F	S	F	S	C	N	Q	E	R	T	B	L	S	A	G	N	A	H
	T	C	Y	Z	B	I	D	W	I	V	N	X	M	Y		N	N	H	A	Q	V
							L	A	F						K	M	S				
							z	w	o						i	x	e				
987	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H	O
	H	T	C	L	P	G	X	T	X	F	K	S	I	R	I	I	D	R	A	D	X
									t	t				m							
988	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H	O	W
	L	O	F	U	T	V	G	T	R	A	J	E	F	F	K	U	U	T	W	L	M
				D		L				K	L	H	T	E	N	F	Z	Q	K	S	
				u		l				l	u	d	w	i	g	x	a	v	e	r	
989	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H	O	W	C
	F	W	Q	I	O	K	S	R	V	P	E	W	C	C	S	Z	G	W	X	I	R
				A		R											N				
				d		i											x				
990	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H	O	W	C	P
	A	R	W	E	Y	P	R	W	D	O	J	N	O	E	A	H	A	R	O	I	H
						N	S	L	G	D	L	O	L	F	W						
						v	i	r	e	i	n	j	x	x	j						
991	V	D	J	Q	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S
	I	L	P	X	U	W	F	W	D	C	I	H	S	U	R	J	R	T	Z	I	W
						J	L	G			E						Q				
						z	w	o			i						i				

TOP SECRET ULTRA

WORK SHEET NO. 9 (CONT'D)

	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
992	D	J	Q	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A
	X	W	T	V	T	T	G	S	V	I	Q	D	M	O	Q	Q	L	S	R	N	K
				C	U	U	L	O	V	E	M	B	W	J			G		H	P	
993	J	Q	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G
	G	L	E	J	O	K	U	I	A	D	J	V	T	A	I	U	B	L	S	A	J
							x	x	x	j	z	z	z	z	z	z	z	z	z	z	z
994	Q	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N
	X	M	Q	T	O	A	R	A	M	L	I	C	Y	D	W	W	U	C	Z	V	T
					n			x	d	r											
995	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A
	Y	I	N	V	O	D	L	B	K	R	T	A	Z	B	J	N	L	N	G	X	C
				e	r	b	e	w	u	s	s	t	e	n	a	s	q	i	n	e	
996	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H
	B	O	M	P	G	B	J	P	O	W	W	Z	A	U	N	H	J	J	D	Y	R
						a				s		q	i								
901	A	D	S	A	A	U	D	B	G	I	U	Y	V	P	Q	I	T	P	S	A	H
				o		t		d	e			e									
902	O	O	W	F	R	L	Z	E	C	Q	U	X	S	Q	J	D	S	Q	D	G	B
						d								t		h	t		x		
903	Z	H	F	K	W	X	Z	A	Y	Z	X	J	V	Q	R	D	U	N	D	H	G
							t				q	e				z	w	n			
904	A	C	V	O	Y	Z	N	N	J	W	J	W	S	J	V	X	J	P	L	L	S
						s				t	l								s		
905	E	B	O	W	A	I	O	R	Z	J	K	D	I	F	E	D	V	N	P	S	E
													e			w	l				

Assumptions:

O - 986/39

LUDWIGXJ 992/33

BEWUSSTE MASQINE 995/35

TOP SECRET ULTRA

WORK SHEET NO. 10

	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
976	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	O	N	A	H
	T	M	E	T	S	O	A	P	I	J	V	A	E	W	D	N	R	Y	L	H	V
					s	q	l	u	e	s	s	e				x					
977	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H	O
	E	L	Q	I	T	V	M	Z	Y	F	B	W			D	Q	C	E	L	N	
								e	s	t				e							
978	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H	O	W
	S	H	C	H	I	Z	Q	F	V	D	M	Q	J	B	I	O	Q	L	C	H	L
					S					O	Q	J	a					G			
					P					G								b			
979	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H	O	W	C
	I	N	D	W	M	Y	R	P	S	X	B	S	I	Z	Y	T	W	X	Z	S	J
								i			d			v							
														s							
980	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H	O	W	C	P
	W	T	S	O	J	Y	R	F	S	J	J	U	Q	G	B	I	R	C	C	A	D
						S	i				n		e								
981	V	D	J	Q	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S
	W	K	V	O	Q	T	U	K	X	I	O	Q	U	V	Y	J	S	F	O	U	Y
						U	I	G	P	E	D	J		Z			H				
						m	a	s	q	i	n	e		a			s				
982	D	J	Q	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A
	H	P	A	H	C	F	T	O	X	K	S	D	O	H	M	C	M	M	Z	B	I
	J				Z	X	K	S	P	A		L									
	d				v	i	k	t	o	r											
983	J	Q	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G
	H	S	Z	V	R	H	B	Z	D	X	N	K	Z	N	O	S	Q	T	H	K	
	J	C	U	C	X	E	W	X	G	N	G	E	H	V	K	L	H	T	E	N	
	J	x	x	j	i	d	k	t	o	n	i	z	e	t	l	u	d	w	i	g	

TOP SECRET ULTRA

30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

985 D K R Z F S F S C N Q E R Y B L S A G N A
Y B O V A O S B G T W X C Q S U V P B R C Y I
V C A O Z B K G D T X C K Q S
V i r a q d t j x x 1

987 R Z F S F S C N Q E R Y B L S A G N A H O
H T C L P G X T U X F K S B I R I I D R A D X
J
z o t t o e

989 F S F S C N Q E R Y B L S A G N A H O W C
F W Q I O K S R V P E W C C S Z G W X I R
A R N
d 1 x

991 V D J Q D K R Z F S F S C N Q E R Y B L S
I L P X U W F W D C I H S U R J R T Z I W
J L G E Q Q
Z W O i n i

TOP SECRET ULTRA

WORK SHEET NO. 10 (CONT'D)

	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	
992	D	J	Q	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	
	X	W	T	V	C	T	U	L	O	I	E	M	B	W	J							
995	J	Q	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	
	G	L	E	J	O	K	U	I	A	I	O	J	V	T	A	I	U	E	I	U	Z	J
994	Q	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	
	X	M	Q	T	O	R	A	M	I	C	X	R	W									
995	D	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	
	Y	Y	N	C	O	D	W	L	L	G	A	Z	N	T	M	L	N	F	G	C		
996	K	R	Z	F	S	F	S	C	N	Q	E	R	Y	B	L	S	A	G	N	A	H	
	B	O	M	P	G	B	J	P	O	W	Z	A	U	N	H	J	J	D	Y	R		
901	A	D	S	A	A	U	D	B	G	I	U	Y	V	P	Q	I	T	P	S	A	H	
902	O	O	W	F	R	L	Z	E	C	Q	U	X	S	Q	J	D	S	Q	D	G	B	
903	Z	H	F	K	W	X	Z	A	Y	Z	X	J	V	Q	R	D	U	N	D	H	G	
904	A	C	V	O	Y	Z	N	N	J	W	J	W	S	J	V	X	J	P	L	L	S	
905	E	B	O	W	A	I	O	R	Z	J	K	D	I	F	E	D	V	N	P	S	E	

Assumptions:

VIKTOR 982/34

JXXJIDATONI 983/30

XXJ 985/40

OTTO 987/37

EI 994/40

[illegible]

TOP SECRET ULTRA

c. RECOVERY OF WHEEL WIRING FOR WHEEL 1

The plain-cipher keyboard pairs were converted to wheel point pairings. The wiring was recovered for all wheels using "A" as the starting point. The ring and grund, however, were known and it would have been just as easy to say that the core position of the first wheel was at "U", the second at "G", the third at "Y" and the UKW at "X".

Position 1
Wheel entry
points

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Q W E R T Z U I O A S D F G H J K P Y X C V B N M L

Position 2
Wheel entry
points

B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
Q W E R T Z U I O A S D F G H J K P Y X C V B N M L

In position 1 the N/A plain-cipher pair on Figure 43 (976 col. 1) was converted to a X/J wheel point pair, P/M (977 col. 1) to R/Y, G/K (978 col. 1) to N/Q, etc. In position 2, the T/D plain-cipher pair on Figure 43 (976 col. 2) was converted to a F/M wheel point pair. The complete compilation of these converted values is shown on Figure 44.

TOP SECRET ULTRA

FIGURE 144

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
1 -	O	K	B	T	I	A	L	D	X	J	U	S	R	F	C	P	F	H	X	B	V	M	R	B	C	X	X
2 -	G	I	J	K	O	L	D	X	J	U	S	R	F	C	P	F	H	X	B	V	M	R	B	C	X	X	X
3 +	D	Y	H	N	M	S	S	Z	Z	R	A	H	X	F	T	S	I	H	Z	E	P	B	M	L	D	V	X
4 +	H	N	M	S	S	Z	Z	R	A	H	X	F	T	S	I	H	Z	E	P	B	M	L	D	V	X	X	X
5 +	N	M	S	S	Z	Z	R	A	H	X	F	T	S	I	H	Z	E	P	B	M	L	D	V	X	X	X	X
6 -	F	P	T	W	F	K	D	P	I	H	A	R	V	Z	F	X	I	R	M	J	T	S	R	N	F	N	O
7 +	M	T	W	F	K	D	P	I	H	A	R	V	Z	F	X	I	R	M	J	T	S	R	N	F	N	O	O
8 -	P	T	W	F	K	D	P	I	H	A	R	V	Z	F	X	I	R	M	J	T	S	R	N	F	N	O	O
9 +	M	T	W	F	K	D	P	I	H	A	R	V	Z	F	X	I	R	M	J	T	S	R	N	F	N	O	O
10 +	I	L	P	W	G	M	S	K	Y	Q	C	D	P	R	B	M	L	E	A	X	I	U	I	B	E	C	K
11 +	J	T	H	I	W	G	M	S	K	Y	Q	C	D	P	R	B	M	L	E	A	X	I	U	I	B	E	C
12 +	X	O	K	J	G	N	W	D	V	N	O	C	F	X	S	O	X	W	L	V	A	J	K	C	Y	K	N
13 -	O	K	J	G	N	W	D	V	N	O	C	F	X	S	O	X	W	L	V	A	J	K	C	Y	K	N	N
14 +	J	T	H	I	W	G	M	S	K	Y	Q	C	D	P	R	B	M	L	E	A	X	I	U	I	B	E	C
15 +	X	O	K	J	G	N	W	D	V	N	O	C	F	X	S	O	X	W	L	V	A	J	K	C	Y	K	N
16 +	O	K	J	G	N	W	D	V	N	O	C	F	X	S	O	X	W	L	V	A	J	K	C	Y	K	N	N
17 +	D	R	F	T	E	D	B	Z	I	H	R	S	O	X	W	L	V	A	J	K	C	Y	K	N	N	N	N
18 -	Q	F	T	E	D	B	Z	I	H	R	S	O	X	W	L	V	A	J	K	C	Y	K	N	N	N	N	N
19 +	Q	F	T	E	D	B	Z	I	H	R	S	O	X	W	L	V	A	J	K	C	Y	K	N	N	N	N	N
20 +	Q	F	T	E	D	B	Z	I	H	R	S	O	X	W	L	V	A	J	K	C	Y	K	N	N	N	N	N
21 +	Q	F	T	E	D	B	Z	I	H	R	S	O	X	W	L	V	A	J	K	C	Y	K	N	N	N	N	N
22 -	B	A	D	C	Q	H	O	T	E	N	Y	M	Z	P	R	T	I	Q	K	O	Y	F	P	T	Q	D	A
23 +	P	X	U	U	C	D	X	Y	P	N	Y	W	I	T	W	R	K	O	Y	F	P	T	Q	D	A	A	L
24 -	S	K	V	F	H	G	F	E	M	U	Y	Q	Z	I	J	H	U	G	F	V	P	T	Q	D	A	A	L
25 +	S	K	V	F	H	G	F	E	M	U	Y	Q	Z	I	J	H	U	G	F	V	P	T	Q	D	A	A	L
26 +	S	K	V	F	H	G	F	E	M	U	Y	Q	Z	I	J	H	U	G	F	V	P	T	Q	D	A	A	L
27 +	B	A	D	C	Q	H	O	T	E	N	Y	M	Z	P	R	T	I	Q	K	O	Y	F	P	T	Q	D	A
28 -	Y	K	E	X	C	S	R	O	M	N	B	Z	I	H	R	S	O	X	W	L	V	A	J	K	C	Y	K
29 +	B	A	V	E	D	M	J	W	K	G	I	Q	F	U	Y	Z	L	S	R	X	N	C	H	T	O	P	O
30 +	B	A	V	E	D	M	J	W	K	G	I	Q	F	U	Y	Z	L	S	R	X	N	C	H	T	O	P	O
31 +	K	S	Z	I	J	P	D	F	A	M	L	R	I	U	B	N	Z	E	P	J	X	W	S	U	O	G	F
32 -	H	Q	G	F	T	D	C	A	S	W	P	T	X	R	F	K	P	U	L	I	R	D	O	G	F	F	N
33 +	B	A	V	E	D	M	J	W	K	G	I	Q	F	U	Y	Z	L	S	R	X	N	C	H	T	O	P	O
34 +	K	S	Z	I	J	P	D	F	A	M	L	R	I	U	B	N	Z	E	P	J	X	W	S	U	O	G	F
35 -	D	U	J	A	I	Z	V	T	E	C	W	P	O	S	M	L	A	P	U	H	M	R	Y	I	B	V	N
36 +	C	X	A	E	D	K	J	S	W	G	F	O	T	Z	L	Q	P	O	I	U	H	S	F	Y	A	N	G
37 +	X	K	E	P	C	V	Z	T	R	L	B	J	N	M	Q	D	O	I	U	H	S	F	Y	A	N	G	G
38 -	X	K	E	P	C	V	Z	T	R	L	B	J	N	M	Q	D	O	I	U	H	S	F	Y	A	N	G	G
39 -	W	S	V	M	I	J	K	Y	E	F	G	R	D	Q	T	Z	N	L	B	O	X	C	A	U	H	P	F
40 +	R	I	M	K	P	H	G	B	U	D	N	C	L	X	E	T	A	Q	J	Y	O	V					

TOP SECRET ULTRA

It was possible to fit the wheel track down the side of Figure 44 by trying all six wheel orders of the Green machine in a test machine, noting at what points "lobsters" occurred with the rings started at DOZL. The only wheel order that satisfied the conditions of "lobsters" in positions 10-11, 17-18, 20-21, 29-30; and 37-38 was what we would have called wheel order R 2 1 3. These numbers were arbitrarily assigned when the Green machine was solved and it was now certain that wheel 1 had 1/ turnovers, wheel 2, 15, and wheel 3, 11 turnovers, because Berlin had stated in message 930 that the wheel order would be R 2 3 1.

Figure 44 was then examined for equidistant patterns and the following were selected for study.

Position	1 12 22	2 13 23
Letter	F G G G	E H H H
	G F F F	H E E E

This equidistant pattern was accepted as evidence that either wheel entry points FE and GH or FH and GE were wired to consecutive positions on the interior face of the wheels. Both situations were examined as follows:

TOP SECRET ULTRA

The pairings produced in columns 3, 4, 5, 7, 9, 10, 11, 14, 15, 16, 17, 18, 20, 21, 23, 25, 26, 28, 30, 31, 33, 35, 36, 37, and 40 were stricken out because of the known wheel track and both situations were examined for repeated pairings. The FE-OH arrangement indicated nothing significant but the FH, GE arrangement showed the following:

GE	FH	MF	RD	SW	HT	XR	DS	WN	QU	TO	EC	CV	ZI	VY	JG	KP
GE	FH		RD	SW	HT		DS						ZI			
GE	FH						DS									

It can be seen that the pairings RD, SW, HT, DS and ZI, in addition to the GE, FH pairing already assumed, are repeated. These repeated pairings were added to the GE, FH in the table shown below, and expanded to derive a complete sequence:

TOP SECRET ULTRA

The columns where turnovers occurred were stricken out and pairs from the table were chained to produce the following sequence:

A L K P B Z I M F H T O X R D S W N J G E C V Y Q U

It was known that the core position of the outside wheel was "U", so if the plain component is completed down to "U", the inner sequence for wheel No. 1 will be found to be:

Core	A	A	L	K	P	B	Z	I	M	F	H	T	O	X	R	D	S	W	N	J	G	E	C	V	Y	Q	U
	B	B	M	L	Q	C	A	J	N	G	I	U	P	Y	S	E	T	X	O	K	H	F	D	W	Z	R	V
	C	C	N	M	R	D	B	K	O	H	J	V	Q	Z	T	F	U	Y	P	L	I	G	E	X	A	S	W
	D	D	O	N	S	E	C	L	P	I	K	W	R	A	U	G	V	Z	Q	M	J	H	F	Y	B	T	X
	E	E	P	O	T	F	D	M	Q	J	L	X	S	B	V	H	W	A	R	N	K	I	G	Z	C	U	Y
	F	F	Q	P	U	G	E	N	R	K	M	Y	T	C	W	I	X	B	S	O	L	J	H	A	D	V	Z
	G	G	R	Q	V	H	F	O	S	L	N	Z	U	D	X	J	Y	C	T	P	M	K	I	B	E	W	A
	H	H	S	R	W	I	G	P	T	M	O	A	V	E	Y	K	Z	D	U	Q	N	L	J	C	F	X	B
	I	I	T	S	X	J	H	Q	U	N	P	B	W	F	Z	L	A	E	V	R	O	M	K	D	G	Y	C
	J	J	U	T	Y	K	I	R	V	O	Q	C	X	G	A	M	B	F	W	S	P	N	L	E	H	Z	D
	K	K	V	U	Z	L	J	S	W	P	R	D	Y	H	B	N	C	G	X	T	Q	O	M	F	I	A	E
	L	L	W	V	A	M	K	T	X	Q	S	E	Z	I	C	O	D	H	Y	U	R	P	N	G	J	B	F
	M	M	X	W	B	N	L	U	Y	R	T	F	A	J	D	P	E	I	Z	V	S	Q	O	H	K	C	G
	N	N	Y	X	C	O	M	V	Z	S	U	G	B	K	E	Q	F	J	A	W	T	R	P	I	L	D	H
	O	O	Z	Y	D	P	N	W	A	T	V	H	C	L	F	R	G	K	B	X	U	S	Q	J	M	E	I
	P	P	A	Z	E	Q	O	X	B	U	W	I	D	M	G	S	H	L	C	Y	V	T	R	K	N	F	J
	Q	Q	B	A	F	R	P	Y	C	V	X	J	E	N	H	T	I	M	D	Z	W	U	S	L	O	G	K
	R	R	C	B	G	S	Q	Z	D	W	Y	K	F	O	I	U	J	N	E	A	X	V	T	M	P	H	L
	S	S	D	C	H	T	R	A	E	X	Z	L	G	P	J	V	K	O	F	B	Y	W	U	N	Q	I	M
New	T	T	E	D	I	U	S	B	F	Y	A	M	H	Q	K	W	L	P	G	C	Z	X	V	O	R	J	N
sequence	U	U	F	E	J	V	T	C	G	Z	B	N	I	R	L	X	M	Q	H	D	<u>A</u>	<u>Y</u>	<u>W</u>	<u>P</u>	<u>S</u>	<u>K</u>	<u>O</u>

This sequence was arbitrarily placed with "A" opposite "A" to represent the wiring for wheel No. 1, thus:

A Y W P S K O U F E J V T C G Z B N I R L X M Q H D
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Wiring for the other wheels was recovered in the same manner as for the Green machine. The complete recovery was:

TOP SECRET ULTRA

R	LDSBFEE	ARPAYWVKGJCUTONIMH
	ABCDEFGHIJKLMN	OPQRSTUVWXYZ
1	AYWPSKDUFEJVTGQZBNIRLXHQHD	ABCDEFGHIJKLMN
	OPQRSTUVWXYZ	ABCDEFGHIJKLMN
2	AEPNZLIDVHJWTCXFRQGBYMQUKS	ABCDEFGHIJKLMN
	OPQRSTUVWXYZ	ABCDEFGHIJKLMN
3	ADYQBNULEHWKPGXFVTZQJHCISR	ABCDEFGHIJKLMN
	OPQRSTUVWXYZ	ABCDEFGHIJKLMN

d. REMOVAL OF THE TWIST

There are 2 types of errors which may be expected to be present in the recovery of "equivalent" wheel wirings.

(a) The wrong sequence of letters may be derived. Consider the sequence placed on the inside face of wheel No. 2:

Recovered sequence:	A E P N Z L I D V H J W T C X F R O G B Y M Q U K S
Equivalent sequence:	B F Q O A M J E W I K X U D Y G S P H C Z N R V L T
	C G R P B N K F X J L Y V E Z H T Q I D A O S W M U

	Z D O M Y K H C U G I V S B W E Q N F A X L P T J R

Any of the 25 other sequences which can be generated by completing the standard alphabet below the recovered sequence would be an equivalent sequence and would work equally well, unless we insist that the wheels be twist free. It should be noted that, with the end wiring, bench mark and starting position of the wheel known, this type of error, i.e. recovery of the incorrect sequence of letters, does not occur in the case of the fast wheel.

(b) The sequence of letters, either correct or an equivalent, may be incorrectly juxtaposed against the standard alphabet sequence representing the outer face of the wheel. With the end wiring, bench mark and starting position of the wheel known, the misplacement of the sequence is the only type of error introduced in the fast wheel recovery.

TOP SECRET ULTRA

Both the (a) and (b) types of errors are generally present in the initial recoveries of the interior wheel wirings.

The 2, 3, 1 wheel order was used in the series of messages which were solved, in which the Ringstellung and Grundstellung used in the encipherment were known. The equivalent wheel wirings were adjusted so that the Ringstellung given was set opposite the core position identified as "Z" on all wheels.

The messages which were solved contained the entire list of Ringstellungen and Grundstellungen with complete instructions for their use so that had we had twist-free wheels we could have read all following messages simply by following the key instructions.

TOP SECRET ULTRA

It was found, of course, that the only messages which could be read, setting the Ringstellung against Z on all wheels, were those in the same wheel order as that used in the messages from which the wheel wiring was recovered.

Partly by trial and error, partly by solution of messages in other wheel orders with cribs and, somewhat belatedly, by utilization of the fixed relationship between any pair of wheels when placed together, the following core positions against which the rings had to be set were recovered for the wheel orders indicated:

R 1 2 3	R 2 3 1	R 3 2 1	R 1 3 2	R 2 1 3	R 3 1 2
Z F Y Y	Z Z Z Z	Z E Y Z	Z F D X	Z Z A Y	Z E E X

Suppose we had recovered only the following:

R 2 3 1	R 3 2 1	R 1 2 3
Z Z Z Z	Z E Y Z	Z F Y Y

We could recover the R 3 1 2 points at which to set the rings by some such reasoning as follows: We know that when wheel No. 3 is placed next to the reflector the ring settings must be placed against ZE on the core so we can say that we must have,

R 3 1 2
Z E

and from the R 2 3 1 we can say that when wheels 3 1 are placed
Z Z Z Z

together in that order the rings must be set at the same letter so that we have R 3 1 2 and from R 1 2 3 we can say that when
Z E E Z F Y Y

wheels 1 2 are placed together in that order the the difference between the points on the core at which the ring settings are placed must be equal to the distance between "F" and "Y". Since we already have "E" for wheel 1, we can say our rings should be set R 3 1 2. The possible extensions of this procedure are apparent.
Z E E X

With the 6 conversions for the ring settings recovered it was considered desirable to remove the twist from the wheels so that Ringstellungen could be set at a constant point, i.e., "Z", on all wheels.

This was accomplished by placing the fast wheel in the original

TOP SECRET ULTRA

solution (Wheel No. 1) in the intermediate or second wheel position and placing one of the other wheels in the first wheel position, as shown in Figure 15. Since we know that when we have the wheel in the first position and we know its starting point, we can recover the correct sequence of letters on the inside face of the wheel, we can then determine the sequence of letters immediately, as will be seen from the following discussion of Figure 15. We can then utilize the fact that we have the correct sequence on the originally recovered now have in the first position.

This statement sounds so involved that it is best clarified by an example.

Suppose we consider Figure 15 in which we show at the left, wheel No. 1 in the first position. At the right of it we show wheel No. 2 in the first position set at "Z", as we have found must be done to produce the condition which we know should be obtained at the "Z" position of the wheel. Above Wheel No. 2 we have placed Wheel No. 1 set at "A" as it must be for the true "Z" position in the 2 1 3 wheel order. Between each two wheels there is placed a separator is the sequence of keyboard letters after passage through the wheels. The sequences underlined are all correct but their placement is very probably incorrect.

Now if we shift wheel 2 to its correct position, "Z" and still require it to deliver CIEZUR etc., to any starting point at the first separator, we must change the lettering on the inside face of the wheel to the sequence shown below.

C I E Z Q Y E J B O U A M F P O L I N V W K D H T S
 Now
 Sequence - T S B E Z R C O V M F I X L Q E Y G W U A P K N D J
 Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
 Q W E R T Z U I O A S D F G H J K P Y I C V B N M L

This corrects the identity of the letters in the sequence on the inside of the wheel but we probably still have it in the wrong position.

If, now, we insist that the CIEZQI etc., sequence pass through wheel No. 1 and deliver the sequence CTDONU etc., somewhere on the

QWERTZUIOASDFGHIJKLPYACVBNML
CTDONUPWYQCGKVERSYFBIAHMLJZ

AYWPSKOUFEJVTGGZBNIRLXMQHD
1 ABCDEFGHIJKLMNOPQ RSTUVWXYZ

QWERTZUIOASDFGHIJKLPYACVBNML
CXEZQYRJEGUAMFOLINVMKDH TS

SRADYQBNUL EHHKKPGAFVVTZOJMC I
3 YZAB CDEFGHIJKLMNOPQRSTUVWXY

QWERTXUIOASDFGHIJKLPYACVBNML

QWERTZUIOASDFGHIJKLPYACVBNML
TWNKXDJVUZSBCRIQEHA YFPGPO

DAYWPSKOUFEJVTGGZBNIRLXMQH
1 ZABCD;FGHIJKLMNOPQRSTUVWXY

QWERTZUIOASDFGHIJKLPYACVBNML

second separator and at the same time require wheel No. 1 to pick up some starting point on the sequence TWINKI etc., from the first separator, as we know it must, since we have had it in the past position at a known starting point, we can slide the sequence CTEZQTR... against the first separator until the letters appearing opposite CTDONUP... form the sequence TWINKI.... which wheel No. 1 is required to pick up.

This can be done quickly and is easier to illustrate than to explain. Consider the following placement of the CTEZQTR sequence against the first separator:

Q W E R T Z U I O A S D F G H J K P Y X C V B N M L
S C X E Z Q Y R J B G U A M F P O L I N V W K D H T

We see that in this placement wheel No. 1 can meet the simultaneous conditions required of it, i.e., that it deliver the keyboard letters CTDONUP etc., to the second separator at the same time it is picking TWINKI etc., from the first separator. The following diagram will make this clear.

First

Separator - Q W E R T Z U I O A S D F G H J K P Y X C V B N M L

Keyboard

Letters - S C X E Z Q Y R J B G U A M F P O L I N V W K D H T

J T S E Z R C O V M F I X L Q H Y G W U A P K N D

Wheel No.3 Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

Keyboard - Q W E R T Z U I O A S D F G H J K P Y X C V B N M L

It is apparent that if we now deliver the CTDONUP sequence through wheel No. 1 we will also deliver the first separator sequence shown below:

1st Separator

Letters: W L N K X D J V U Z S B C R I Q E H A Y F M G P O T

Keyboard

Letters: C T D O N U P W Y Q G K V E R S X F B I A H M L J Z

To deliver the sequence CXEZQY...to the desired point at the first separator we must slide the corrected inner sequence to the position shown by the underlined sequence in the above Figure.

TOP SECRET U.S.

To remove the twist from wheel No. 2, we prepare a chart showing the action for this wheel in the fast position with wheel No. 1 in the next interior position. This is shown in Figure 46.

Examination of Figure 46 with the same considerations in mind as for Figure 45 reveals that, to deliver the sequence NGVRIY etc., to the first separator, through wheel No. 2 in the "Z" position, we must re-letter the inner sequence as follows:

```

  N G V R I Y K E H D U M S F L B Z Q O C P A T W J X
  W M U C G R P B N K F X J L Y V E Z H T Q I D A O S
  Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
  Q W E R T Z U I O A S D F G H J K P Y X C V B N M L

```

If, now, we require wheel No. 1 to deliver the sequence of letters LKUZGNY etc., to the second separator while wheel No. 1 is picking up TWLNKI etc., from the first separator we see that we must place the sequence NGVRIY etc., against the first separator as follows:

```

  Q W E R T Z U I O A S D F G H J K P Y X C V B N M L
  A T W J X N G V R I Y K E H D U M S F L B Z Q O C P

```

This in turn requires the following placement of the corrected inner sequence of wheel No. 2 as follows:

```

  Q W E R T Z U I O A S D F G H J K P Y X C V B N M L
  A T W J X N G V R I Y K E H D U M S F L B Z Q O C P

  I D A O S W M U C G R P B N K F X J L Y V E Z H T Q
  Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

  Q W E R T Z U I O A S D F G H J K P Y X C V B N M L

```

To remove the twist from wheel No. 1 we prepare a chart for this wheel in the fast position with the now twist free wheel No. 3 in the next interior position. This is shown in Figure 47.

We examine this figure together with Figure 46, in which we see that when wheel No. 3 is in the fast position it picks up the keyboard sequence CXEZQY etc. We are required, then, to place the TWLNKX wheel No. 1 sequence against the first separator in such a

LKUZGNYQBJVAVWDIFECHSRXTPOM

1 SKOUFEJVTGZBNIRLXMQHDA YWP
EFGHIJKLMNOPQRSTU VWXYZ ABCD

QWERTZUIOASDFGHJKPYXC VBNML
NGVRIYKEHDUNSLBZQOCPATWJX

UKSAEPNZLIDVHJWTCXFR OGBYMQ
XYZABCDEFGHIJKLMNOPQR STUVW

QWERTZUIOASDFGHJKPYXC VBNML

TWLNKXDJVUZSBCRIQEHAYFMGPQ

DA YWPSKOUFEJVTGZBNIRLXMQH
Z ABCDEFGHIJKLMNOPQR STUVWXY

QWERTZUIOASDFGHJKPYXC VBNML

QWERTZUIOASDPGHIJKPXYICVBNML
 HWKQELRFBXVGSQJPDWYITNZCMUA
 KADYQBNULENHWKPGXFVVTZOJMCIS
 ZABCDEFGHIJKLNMOPQRSITUWXY
 QWERTZUIOASDPGHIJKPXYICVBNML
 TWLNKXDJVUZSBCRIQEHAYFPMGPO
 DAYWPSKOUFEJATCGZBNIRLIMQH
 ZABCDEFGHIJKLNMOPQRSITUWXY
 QWERTZUIOASDPGHIJKPXYICVBNML

3

1

QWERTZUIOASDPGHIJKPXYICVBNML
 JTSBEEZRCOVWFIILNMO.PQRSITUWXY
 ZABCDEFGHIJKLNMOPQRSITUWXY
 QWERTZUIOASDPGHIJKPXYICVBNML
 1 ZABCDEFGHIJKLNMOPQRSITUWXY
 QWERTZUIOASDPGHIJKPXYICVBNML

1

TOP SECRET ULTRA

way that a portion of the HWKOEL etc., sequence falls against CXYZQ on the separator. This condition is fulfilled if we slide our inner sequence for Wheel No. 1 to the position indicated below.

(3) QWERTZUIOASDFGHJKPXYCVBNML
UAHWKOELRFBXVGSQJPD MUTNZCN

JTSBEZRCOV MFI XLQHYGWUAPKND
 ZABCDEFGHIJKLMNOPQRSTUVWXYZ

(1) QWERTZUIOASDFGHJKPXYCVBNML
OTWLNKXDJVUZSBCRIQEHAYFMGP

HDAIWPSKOUFEJVT CGZBNIRLXMQ
 ZABCDEFGHIJKLMNOPQRSTUVWXYZ

QWERTZUIOASDFGHJKPXYCVBNML

The twist free wirings for wheels 1, 2, 3 then are as follows:

No. 1 DAYWPSKOUFEJVT CGZBNIRLXMQH
 ABCDEFGHIJKLMNOPQRSTUVWXYZ

No. 2 DAOSWMUCGRPB NKFXJLYVEZH TQI
 ABCDEFGHIJKLMNOPQRSTUVWXYZ

No. 3 TSBEZRCOV MFI XLQHYGWUAPKNDJ
 ABCDEFGHIJKLMNOPQRSTUVWXYZ

The Umkehrwalze, it will be noted, was twist free.

TOP SECRET ULTRA

PART II, D. ENIGMA: DETERMINATION OF THE USE OF WHEELS
ON UNSOLVED CIRCUITS

1. MULTIPLE TURNOVER WHEELS. 4-0 BERLIN-MADRID

About 5 May, 1941, the 4-0 Circuit ceased using double transposition. A single letter frequency count, followed by an application of the Log Odds Test, identified the new system as Enigma encipherment. This was one of the most successful system identifications achieved by the employment of the Log Odds Test.

An examination of the traffic on a single day revealed that messages from the same transmitting agent could be superimposed in depth by use of the time group. For example, a message having the preamble encipherment time 1410 would be in phase from the 11th letter of a message having the encipherment time 1400.

This method of indication was similar to that previously encountered only in the Western Hemisphere, namely, in the 3-N group, Argentine-Berlin: a secret number, which changed daily, was added to the selected encipherment time; the machine was then advanced that number of positions forward from the basic Grund established for the day.

After determining the foregoing, the various Enigmas employed by the Sicherheitsdienst group, of which 4-0 was a part, were considered. There had been only four machines employed by this group--The Green, The Red, a combination of Red wheels and Green reflector, and the M machine. Since the Red and Green machines had the 11-15-17 turnover pattern plus the rotating reflector--which produces the "lobster" effect, a study was made of the chance lobsters and actual lobsters on both the stationary and rotating type reflectors. In the samples examined the non-lobstering machine produced a higher lobster count than the true rotating reflector. Hence it was concluded that a lobster count would not serve to distinguish between multiple and single turnover machines.

Assuming then, that the traffic was enciphered on one of the known machines, a considerable time was expended on guesses in depth--the depth of any series of messages was never enough to yield a solution on that method alone--then running menus on the sliding grenade and checking the resultant hits in the uncribbed depth.

TOP SECRET ULTRA

This method eventually read the traffic in a depth of 12 messages. The successful crib was DREI producing in the depth such excellent combinations as ERDE; EMIS; AMGE, etc. These were easily expanded and the full text recovered. The machine involved employed the Red wheels and the Green reflector.*

The plain text of these messages provided cribs which were successfully used in the solution of a considerable volume of the remaining traffic. Seven of the 12 messages had the combination of letters XJJANX, followed by the name of the addressee. This crib appeared in the beginning of each message after a four or five-letter dummy word. The simple expedient of assuming this same combination at the beginning of all messages, then running menus on the sliding grenades and checking the "hits", resulted in reading over 90% of the traffic on hand.

* The only instance known up to this time of a machine using Red wheels and Green reflector was the case of the super-enciphered instructions for the Red machine when first sent to Argentina. The Berlin message of 5 December, 1943, saying "We got the machines mixed up here", was interpreted at the time as meaning Berlin had misused some one element, such as inadvertently picking up a wheel from a different Zigma. As facts developed later, however, the statement "We got the machines mixed up" probably meant, simply, that the wrong machine was used.

TOP SECRET ULTRA

PART II, D.

2. STECKER. 4-I HAMBURG-BORDEAUX

In the period immediately preceding the change from the hand to machine system, several 4-I messages were solved which were re-encipherments of unidentified cipher text traffic. These had a short plain text internal preamble giving a serial number, letter count, and a cover name to identify the enciphered traffic.

An analysis of the plain-text messages deciphered in the old system showed that some type of radio intercept activity was involved. One message spoke of installing rhombic antennae, another spoke of guarding certain frequencies at specified times, and another gave the signal strength of radio intercepts. From this information it was deduced that the Bordeaux end of the 4-I circuit acted as a sort of monitoring and relay station which listened in to certain out-stations for the Hamburg control and furnished Hamburg with the text of an out-station message in the event that Hamburg failed to receive it.

The machine traffic was characterized by a three letter doubly enciphered indicator which appeared as the first six letters of the message. This was identified by the familiar throw-on effect produced by double encipherment. A three letter indicator was unknown in Coast Guard experience with Enigma traffic. Further information about the machine was secured through a re-cipher on the part of Bordeaux. 10 groups of a message were sent; then the transmission was interrupted and a message was later sent which repeated the 10 groups with most of the letters being identical. The letters which were not identical were substituted in such a manner as to suggest that a stecker had been employed and that one or perhaps two wires had been improperly plugged. The combination of the stecker and the three letter indicator strongly suggested the German Service wheels.

The next step in the analysis was the identification of the traffic re-enciphered in the last days of the old hand system. This was shown to be the 2-C circuit, which was F.B.I. controlled, between New York and Hamburg. It was then possible by examining message lengths and transmission times to find days on which Bordeaux had re-enciphered the New York end of the 2-C by machine and relayed it to Hamburg. Message placements were found by

TOP SECRET ULTRA

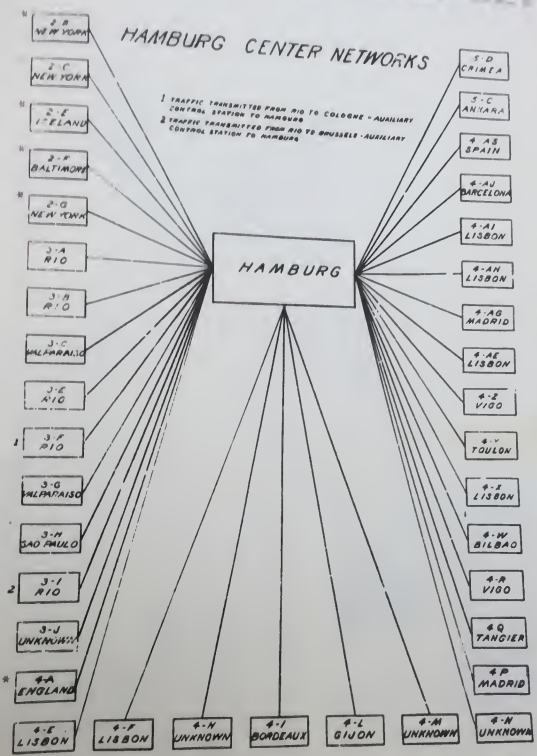
sliding strips of the two cipher texts against each other. A New York message of about 250 letters was slid against a 4-I message approximately 60 letters longer, until a position was reached which produced no conflicts. Correct placements supplied a 250 letter crib. Solution was produced by trial of these cribs on the Bombe. The 4-I machine proved to be the Service wheels 1, 2, 3 with the fixed Bruno reflector and stecker.

From a security standpoint, the conditions under which circuit 4-I operated exhibited an almost complete abandonment of good cryptographic practice. Not only did the Germans use their highest security machine to re-transmit low grade traffic, but the grundstellungen used were those employed on Spanish Abwehr networks. Furthermore, there was every indication that the Germans were aware that the New York circuit was controlled; yet the re-encipherment of the cipher text of this low grade traffic was permitted. It is interesting to speculate as to why Oberinspektor Menzer permitted the arrangement used in Circuit 4-I. Furthermore, it is the only example known to this office of the Service machine being employed for clandestine traffic.

TOP SECRET ULTRA

HAMBURG CENTER NETWORKS

1 TRAFFIC TRANSMITTED FROM RIO TO COLOGNE - AUXILIARY
CONTROL STATION TO HAMBURG
2 TRAFFIC TRANSMITTED FROM RIO TO BRUSSELS - AUXILIARY
CONTROL STATION TO HAMBURG



*"Controlled"

